ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

27 MAGGIO 2020

federalismi.it

Fascicolo n. 16/2020

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

ISSN 1826-3534
Numero 16, 2020
Tutti i contributi, ad eccezione dell'editoriale di apertura, sono stati sottoposti a *double blind peer review*.

E-mail: redazione@federalismi.it

Sommario

ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

27 MAGGIO 2020

Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione

di Fernanda Faini
Professore a contratto di Diritto e nuove tecnologie
Università Telematica Internazionale Uninettuno

Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione *

di Fernanda Faini
Professore a contratto di Diritto e nuove tecnologie
Università Telematica Internazionale Uninettuno

Abstract [It]: Alla luce del quadro giuridico europeo e nazionale di riferimento, il contributo intende esaminare il rapporto che lega diritto e tecnica attraverso l'esame di alcune tecnologie emergenti, quali l'intelligenza artificiale, la *blockchain* e lo *smart contract*. A tal fine, il lavoro analizza le principali caratteristiche tecniche e le problematiche giuridiche maggiormente rilevanti, evidenziando nei casi oggetto di esame gli aspetti critici più significativi dell'interazione tra tecnologia e diritto. In considerazione dell'analisi svolta, il contributo delinea strumenti utili per affrontare le problematiche emerse e disegnare un'evoluzione della regolazione giuridica basata sul correlato mutamento del rapporto tra diritto e tecnologia: la direzione suggerita si concretizza nell'approccio preventivo e proattivo dell'incorporazione del diritto nella tecnica, accompagnato dall'attribuzione del diritto alla comprensibilità e alla contestabilità della tecnologia e da una logica di responsabilizzazione dei soggetti.

Abstract [En]: In the light of the European and national legal framework of reference, the contribution intends to examine the relationship between law and technology through the examination of some emerging technologies, such as artificial intelligence, blockchain and smart contracts. To this end, the paper analyzes the main technical characteristics and the most relevant legal problems, pointing out in the cases under examination the most significant critical aspects of the interaction between technology and law. In consideration of the analysis carried out, the contribution outlines useful tools to deal with the issues that emerged and to draw an evolution of the legal regulation based on the related change in the relationship between law and technology: the suggested direction takes shape in the preventive and proactive approach of incorporating the law into the technique, accompanied by the attribution of the right to the comprehensibility and contestability of the technology and by a logic of accountability.

1. Il rapporto tra diritto e tecnologia

L'evoluzione tecnologica incide profondamente sulla vita dell'uomo; le tecnologie, iniziale ausilio delle attività umane, nel corso del tempo sono state capaci di determinare una profonda trasformazione nella stessa esistenza individuale e collettiva, accompagnata dall'emersione di nuove esigenze e dall'impatto sulle attività, sulle relazioni, sulla crescita sociale ed economica, sul modo di pensare dell'uomo.

In tale mutato contesto, il diritto è chiamato ad occuparsi di questi fenomeni, dovendo riuscire a regolare la tecnologia e a bilanciare gli interessi, proteggere i diritti, prevenire e risolvere i conflitti[1].

* Articolo sottoposto a referaggio. Il presente saggio è frutto delle riflessioni svolte nelle attività dell'Unità di ricerca "*Babel - Blockchains and Artificial Intelligence for Business, Economics and Law*" dell'Università degli Studi di Firenze.

[1] In merito all'impatto dell'evoluzione tecnologica sul diritto e sui diritti cfr., *inter alia*, C. FARALLI, *Diritti e nuove tecnologie*, in *Tigor. Rivista di scienze della comunicazione e di argomentazione giuridica*, fasc. 2, 2019, pp. 43-52: «per i giuristi si è posto il problema se e come fissare delle regole senza soffocare i progressi della scienza, ma anche senza ledere i diritti

Per comprendere il rapporto tra diritto e tecnologia che caratterizza la società contemporanea, dominata dalle cosiddette tecnologie emergenti, è necessario volgere lo sguardo brevemente alla storia che caratterizza questa relazione e il correlato bisogno di regolazione dell'informatica.

Fin dall'avvento dell'informatica sono emerse questioni giuridiche, conseguenti all'impatto e all'applicazione delle tecnologie informatiche nella società.

Il diritto dell'informatica, che nasce quando iniziano la riflessione giuridica e la produzione di norme che riguardano le tecnologie informatiche, ha un'evoluzione rapida, estesa e profonda, involgendo numerosi ambiti del diritto[2].

Negli anni '60 la prima problematica che il diritto si trova ad affrontare riguarda il "cuore" della tecnologia: la tutela giuridica del software, che comincia a diventare oggetto di contratti e la cui protezione giuridica oscilla tra le contrapposte soluzioni della tutela brevettuale e del diritto d'autore, opzione che si consolida come soluzione privilegiata in diversi Stati negli anni '80[3].

Già negli anni '70 il diritto affianca alla protezione della tecnologia attraverso la tutela del software la protezione dell'uomo rispetto alla tecnologia, in specifico la tutela della persona attraverso la protezione dei dati personali nei confronti dei pericoli dell'elaborazione automatica dei dati[4].

Accanto a questa esigenza costante di tutelare l'uomo rispetto alle possibilità tecnologiche attraverso la protezione dei suoi dati, fin dal suo avvento e, ancor più, con la diffusione di Internet, il rapporto tra tecnologia e diritto si caratterizza per ulteriori profili, che ancora oggi costituiscono nodi cruciali: la necessità di costruire una *governance* efficace e la vocazione transnazionale dei problemi, accompagnata dalla correlata necessità di garantire omogeneità nelle risposte offerte dai diversi ordinamenti. Tali profili conseguono strettamente all'esigenza di una regolazione capace di disciplinare in modo adeguato l'evoluzione tecnologica.

Sotto il primo profilo, fin dagli anni '90 emerge prepotentemente l'esigenza di costruire una *governance*

---

degli individui»; C. FARALLI (a cura di), *Vulnerabilità e nuove tecnologie*, in *Notizie di Politeia*, n. 136, 2019, pp. 5-108; M. TALLACCHINI, *Diritto e scienza*, in B. MONTANARI (a cura di), *Luoghi della filosofia del diritto. Idee strutture mutamenti*, Torino, 2012, pp. 145-169; S. AMATO, *Scienza tecnologia e diritto*, in B. MONTANARI (a cura di), *Scienza tecnologia & diritto (ST&D)*, Milano, 2006, pp. 51-64.

[2] Il rapporto tra informatica e diritto ha determinato due dimensioni connesse e complementari dell'informatica giuridica: quella dell'informatica del diritto (informatica giuridica in senso stretto), che attiene all'utilizzo dell'informatica nelle attività giuridiche, e quella del diritto dell'informatica (informatica giuridica in senso lato), che riguarda le problematiche giuridiche sorte dall'informatica. Per designare l'informatica giuridica Losano usa nel 1969 il termine "giuscibernetica" e Frosini nel 1975 il termine "giuritecnica": M.G. LOSANO, *Giuscibernetica. Macchine e modelli cibernetici nel diritto*, Torino, 1969; V. FROSINI, *La giuritecnica: problemi e proposte*, in *Informatica e diritto*, fasc. 1, 1975, p. 26 ss. Al riguardo cfr. G. ALPA, *L'applicazione delle tecnologie informatiche nel campo del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 1996, p. 515; R. BORRUSO, voce *Informatica giuridica*, in *Enc. dir.*, agg., I, Milano, 1997, p. 640 ss.; G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, II ed., Torino, 2010, p. 13 ss.

[3] Negli anni '80 emergono le prime controversie aventi ad oggetto il software e sono prodotte le prime disposizioni normative.

[4] Cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, cit., p. 34 ss.

efficace ed effettiva con l'istituzione di soggetti dotati di indipendenza e chiamati ad occuparsi della tutela di diritti e del bilanciamento tra interessi diversi: con il d.lgs. 39/1993 viene istituita l'Autorità per l'informatica nella Pubblica Amministrazione (AIPA)[5], con la legge 675/1996 prende vita il Garante per la protezione dei dati personali e con la legge 249/1997 nasce l'Autorità per le garanzie nelle comunicazioni (AGCOM).

Sotto il secondo profilo, insieme a questa esigenza di *governance*, si manifesta fin dagli anni '90 l'impulso sovranazionale del legislatore europeo, cui conseguono in Italia numerosi e significativi atti normativi[6].

Lo stimolo sovranazionale, unito all'esigenza di *governance*, spinge nel nuovo millennio, in parallelo con la maggiore pervasività delle tecnologie informatiche nella vita umana, a regolare in modo sistematico e organico interi ambiti di disciplina: vengono emanati codici e testi unici[7], accompagnati dalla produzione di normativa di rango secondario, regole tecniche e provvedimenti delle autorità indipendenti, istituite per rispondere al bisogno di governare la tecnologia[8]. In questa proliferazione normativa emerge e cresce nel corso degli anni l'esigenza di soluzioni condivise a livello sovranazionale; molte norme italiane sono di derivazione europea e, in tale materia, aumentano gli atti a livello internazionale: la normativa italiana, seppur in continua trasformazione e poco organica, recepisce i continui impulsi sovranazionali.

Nell'evoluzione tecnologica, accanto alla *governance* e alla vocazione transnazionale, rileva un altro aspetto particolarmente significativo, che caratterizza anche la contemporanea società dominata dalle tecnologie emergenti: lo sviluppo di Internet e, ancor più, del *web 2.0* delinea un modello di produzione paritetica, orizzontale e collaborativa, che si affianca ai consolidati modelli verticali basati sul controllo di un'autorità centrale, generando nuove opportunità, ma anche inedite problematiche giuridiche[9].

Nella storia che caratterizza il rapporto tra diritto e tecnologia emerge il dialogo difficile, ma imprescindibile tra norme giuridiche e regole informatiche, ossia le regole applicate dal codice informatico (cosiddetta *lex informatica* o *digitalis*), che hanno la capacità di condizionare i comportamenti umani, dal

[5] Negli anni è diventata Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), ai sensi dell'art. 176 del d.lgs. 196/2003, DigitPA, a seguito del d.lgs. 177/2009, e attualmente Agenzia per l'Italia digitale (AgID), ai sensi degli artt. 19-22 del d.l. 83/2012 convertito con modificazioni dalla legge 134/2012.

[6] Esemplificativamente il d.lgs. 518/1992, che modifica la legge sul diritto d'autore (legge 633/1941), in attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore, seguito qualche anno dopo dal d.lgs. 169/1999, che modifica nuovamente la legge 633/1941, in attuazione della direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati; la legge 675/1996, in attuazione della direttiva 96/45/CE in materia di protezione dei dati personali; il d.lgs. 185/1999, che disciplina i contratti telematici, in attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza.

[7] Esemplificativamente il Codice in materia di protezione dei dati personali (d.lgs. 196/2003); il Codice delle comunicazioni elettroniche (d.lgs. 259/2003), in attuazione delle relative direttive europee; la normativa sul commercio elettronico (d.lgs. 70/2003), in attuazione della direttiva 2000/31/CE; il Codice dell'amministrazione digitale (d.lgs. 82/2005); il Codice della proprietà industriale (d.lgs. 30/2005).

[8] Cfr. G. ZICCARDI, *Il computer e il giurista*, Milano, 2015, p. 4 ss.

[9] Cfr. G. SARTOR, *Internet e il diritto*, in C. DI COCCO, G. SARTOR (a cura di), *Temi di diritto dell'informatica*, II ed., Torino, 2013, p. 1 ss.

momento che abilitano azioni e interazioni e vi collegano effetti. Più ampiamente la *lex informatica* condiziona ogni altra forma di regolazione, compresa quella giuridica, e l'uomo, per mezzo dello strumento del diritto, deve essere capace di governarla, raggiungendo un difficile equilibrio, idoneo a non limitare l'evoluzione tecnica e, allo stesso tempo, capace di non determinare la prevalenza della tecnologia sulla regolazione giuridica[10]. Questo bilanciamento tra il ruolo del diritto e le potenzialità tecnologiche è indispensabile, non solo perché altrimenti il diritto non svolgerebbe la funzione di regolazione cui è chiamato, ma anche perché rischierebbe di votarsi all'inefficacia e al mancato rispetto nella realtà concreta. Proprio alla luce del rapporto che lega diritto e tecnica, risultano di particolare interesse alcune tecnologie emergenti, oggetto di analisi in questo contributo: l'intelligenza artificiale, per cui si può parlare di *lex robotica*, dove il diritto è chiamato a governare la tecnologia e, in specifico, dati e algoritmi; la *blockchain*, definita *lex cryptographia*[11], che trasforma il modo di scambiarsi valore e muta i meccanismi di fiducia (detta per questo anche Internet *of value*)[12]; lo *smart contract*, applicazione della *blockchain*, in cui norme giuridiche e regole informatiche si intersecano significativamente, determinando esigenze e problematiche inedite.
Il contributo intende esaminare il rapporto tra diritto e tecnica, attraverso l'esame di tali tecnologie emergenti, analizzandone le caratteristiche tecniche e le più rilevanti problematiche giuridiche. Il lavoro intende evidenziare gli aspetti critici dell'interazione tra tecnologia e diritto e ipotizzare strumenti utili per affrontarli, capaci di determinare un'evoluzione della regolazione giuridica basata sul correlato mutamento del rapporto tra diritto e tecnologia.

2. Le caratteristiche tecniche e i profili giuridici delle tecnologie emergenti

2.1. Intelligenza artificiale

L'intelligenza artificiale ha acquisito il ruolo di protagonista nella contemporanea società tecnologica, in considerazione delle possibilità e dei vantaggi che garantisce sia nel contesto privato sia in quello pubblico[13].

[10] Al riguardo cfr. G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, cit., p. 37 ss.; G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2012, pp. 831-840; E. MAESTRI, Lex informatica *e* soft law. *Le architetture normative del cybespazio*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, Milano, 2017, pp. 157-177; G. CORASANITI, *Il diritto nella società digitale*, Milano, 2018; M. GIULIANO, *La blockchain e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, in *Il diritto dell'informazione e dell'informatica*, fasc. 6, 2018, p. 989 ss.
[11] A. WRIGHT, P. DE FILIPPI, *Decentralized Blockchain Technology and the Rise of* Lex Cryptographia, in *https://ssrn.com/abstract=2580664*, 2015, pp. 1-58.
[12] Se Internet ha trasformato il modo di scambiarsi informazioni e connettersi agli altri, la *blockchain* trasforma il modo di scambiarsi valore. Cfr. M. GIULIANO, *op. cit.*, p. 989 ss.; M. CASTELLANI, P. POMI, C. TIBERTI, A. TURATO, *Blockchain. Guida pratica tecnico giuridica all'uso*, Firenze, 2019, p. 16 ss.
[13] Sull'impatto e sulle implicazioni dell'intelligenza artificiale cfr., *inter alia*, M. TEGMARK, *Vita 3.0. Essere umani nell'era dell'intelligenza artificiale*, trad. it., Milano, 2018; P. BENANTI, *Le macchine sapienti. Intelligenze artificiali e decisioni umane*, Bologna, 2018. Sui profili etici, filosofici e giuridici dell'intelligenza artificiale cfr. E. ANCONA (a cura di), *Soggettività,*

L'analisi delle caratteristiche tecniche è necessaria al fine di poter esaminare gli aspetti giuridici e, correlativamente, l'evoluzione del rapporto tra diritto e tecnologia.

Il termine intelligenza artificiale si riferisce alla capacità della macchina di «riprodurre o attuare operazioni tipiche delle funzioni cognitive umane, quali per esempio l'apprendimento, il *problem solving*, il riconoscimento di volti, la traduzione del linguaggio, etc.»[14].

L'Unione europea include nella definizione di intelligenza artificiale (IA) «sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»: i sistemi basati sull'intelligenza artificiale possono consistere in «software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale)» oppure «incorporare l'IA in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'Internet delle cose)»[15].

Come emerge dalle definizioni, il concetto di intelligenza artificiale abbraccia al suo interno sistemi molto diversi, che però presentano alcune caratteristiche tecniche comuni: per sviluppare soluzioni di intelligenza artificiale sono necessari ingenti volumi di dati, che sono elaborati da algoritmi, al fine di raggiungere il risultato cui le soluzioni di intelligenza artificiale sono rivolte.

Di conseguenza, l'anima delle soluzioni di intelligenza artificiale è costituita da enormi insiemi di dati, i *big data*[16], e da algoritmi e reti neurali artificiali, capaci di "animare" i dati a disposizione e di estrarne il

responsabilità, normatività 4.0. Profili filosofico-giuridici dell'intelligenza artificiale, in *Rivista di Filosofia del diritto*, fasc. 1, 2019, pp. 81-142; A. D'ALOIA (a cura di), *Intelligenza artificiale (contributi del Convegno su "Intelligenza artificiale e diritto. Come regolare un mondo nuovo", Parma, 12 ottobre 2018)*, in *BioLaw Journal*, fasc. 1, 2019, pp. 3-182; P. MORO, *Intelligenza artificiale e professioni legali. La questione del metodo*, in *Journal of Ethics and Legal Technologies*, n. 1, 2019, pp. 24-43. La presente analisi sull'intelligenza artificiale tiene in considerazione le riflessioni contenute in F. FAINI, *La* governance *dell'intelligenza artificiale tra etica e diritto*, in *Notizie di Politeia*, fasc. 1, 2020, pp. 59-82.

[14] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di Filosofia del diritto*, fasc. 1, 2019, p. 88.

[15] Comunicazione della Commissione europea «*L'intelligenza artificiale per l'Europa*» COM(2018) 237 *final* del 25 aprile 2018.

[16] I *big data* consistono in enormi volumi di dati, provenienti da fonti diverse e analizzati per mezzo di algoritmi, *data mining*, *big data analytics*, *machine learning* e altre tecniche. I *big data* si caratterizzano per il volume (capacità di acquisire, memorizzare, accedere ed elaborare enormi quantità di dati), la varietà (l'eterogeneità della tipologia e dei formati dei dati, provenienti da fonti diverse), la velocità (capacità di acquisizione e analisi in tempo reale o ad alta velocità) e, secondo alcuni, anche il valore (il valore dei *big data* come insieme) e la veracità o veridicità (la qualità e l'accuratezza dell'analisi). Su algoritmi e diritto cfr. P. MORO, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, in *Rivista di Diritto dei media*, fasc. 3, 2019, pp. 11-22. Su *big data* e algoritmi cfr., *inter alia*, V. MAYER-SCHÖNBERGER, K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, trad. it., Milano, 2013; G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018; A.C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di Filosofia del diritto*, fasc. 1, 2019, pp. 107-124; M. DELMASTRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019; sia consentito, altresì, il rinvio a F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019. Sui problemi relativi alla "datificazione" cfr. A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Il diritto dell'informazione e dell'informatica*, fasc. 2, 2019, p. 442 ss.

valore, basandosi su correlazioni, inferenze e metodologie deterministiche, raggiungendo in tal modo significativi ed eterogenei obiettivi[17].

L'approccio su cui è basata l'intelligenza artificiale non è fondato su spiegazioni causali e logico-deduttive, dal momento che si affida a connessioni e inferenze tra dati e poggia sulla probabilità: è distante dalla logica tipica del ragionamento umano, basata su ipotesi predeterminate e nessi di causalità, determinando talvolta difficoltà di comprensione circa le motivazioni (il "perché") delle risposte fornite[18].

Il "valore" che è possibile estrarre dai dati grazie agli algoritmi consiste nella conoscenza e assume diverse declinazioni, quali l'interpretazione dei bisogni, la profilazione degli utenti, il supporto alle decisioni, l'ottimizzazione dei processi. Dal momento che elevate correlazioni tra i dati indicano alte probabilità, la conoscenza può non limitarsi al passato e al presente, ma estendersi al futuro, determinando una capacità predittiva[19], che consente di fare previsioni sugli andamenti di mercato, indicare preventivamente l'usura di infrastrutture, migliorare diagnosi e cure, prevenire disastri, prendere decisioni politiche[20]. A tali funzioni, l'intelligenza artificiale affianca la possibilità di essere proficuamente impiegata nello svolgimento di attività e nell'erogazione di servizi, garantendo maggiore efficacia ed efficienza, assicurando tempestività e consentendo risparmi in termini finanziari e umani, determinando la trasformazione dei servizi, la semplificazione delle procedure e la migliore interazione con gli utenti (ad esempio, facendo uso di *chatbot* e assistenti digitali).

Come emerge dalle finalità perseguibili con sistemi di intelligenza artificiale, l'utilizzo della conoscenza e delle predizioni e le eterogenee possibilità di impiego in attività e servizi rispondono sicuramente alla realizzazione di vantaggi economici cui sono diretti i soggetti privati, ma anche alla tutela di interessi

[17] Cfr. A. MANTELERO, *Big data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012, fasc. 1, pp. 135-144; G. SARTOR, M. VIOLA DE AZEVEDO CUNHA, *Il caso Google e i rapporti regolatori USA/EU*, in *Il diritto dell'informazione e dell'informatica*, 2014, fasc. 4-5, pp. 657-680; L. AVITABILE, *Il diritto davanti all'algoritmo*, in *Rivista Italiana per le Scienze Giuridiche*, fasc. 8, 2017, pp. 315-327; A.C. AMATO MANGIAMELI, *op. cit.*, p. 107 ss.

[18] In tal senso A. SIMONCINI, S. SUWEIS, *op. cit.*, p. 92: in un approccio logico-deduttivo si pone un problema, si formalizza matematicamente e poi si traduce in un algoritmo, mentre in un approccio statistico la macchina "impara" direttamente dai dati, ma non si conosce la *ratio* delle risposte. Cfr., altresì, C. CASONATO, *Intelligenza artificiale e diritto costituzionale: prime considerazioni*, in *Diritto pubblico comparato ed europeo*, numero speciale, 2019, pp. 101-130; A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, in *Rivista trimestrale di diritto pubblico*, fasc. 4, 2019, p. 1149 ss. Al riguardo cfr. P. MORO, *Algoritmi e pensiero giuridico. Antinomie e interazioni*, cit., p. 19: «le procedure formali di apprendimento automatico restano inferenze ipotetiche e non possono interpretare o risolvere problemi complessi della vita reale, come i conflitti di valore, che manifestano costante variabilità ed incertezza e che sono difficili da codificare attraverso misurazioni o funzioni numeriche»; di conseguenza, «la possibilità di stabilire un'analogia tra stato mentale e logica della macchina avviene solo sul piano dell'accettabilità dei risultati e non della identità delle procedure di ragionamento e di decisione: tali metodologie sono riferibili propriamente soltanto all'uomo e sono radicalmente differenti nel calcolatore che, tuttavia, può arrivare ai medesimi esiti dimostrativi».

[19] Cfr. V. MAYER-SCHÖNBERGER, K. CUKIER, *op. cit.*, p. 73 ss.

[20] Cfr., *inter alia*, A. MANTELERO, *op. cit.*, pp. 138-139.

generali, alla cui realizzazione sono orientati i soggetti pubblici[21].

Le caratteristiche tecniche dell'intelligenza artificiale determinano, però, una serie di problematiche per il diritto, dovute sia ai rischi relativi alla logica inferenziale e deterministica, sia al fatto che tale approccio ontologicamente rischia di scontrarsi con norme e principi giuridici.

In primo luogo, in considerazione delle caratteristiche tecniche, l'utilizzo dell'intelligenza artificiale si trova a fare i conti con la natura inferenziale e probabilistica delle elaborazioni compiute dagli algoritmi stessi. Qui si annida un primo significativo aspetto problematico: l'analisi dei dati può condurre a conclusioni imprecise e discriminatorie, laddove i dati non siano debitamente annotati, in modo da poter essere correttamente utilizzati e interpretati dalla macchina. L'intelligenza artificiale, infatti, si serve di quei dati per "imparare", per individuare e far emergere correlazioni: per farlo ha bisogno di una significativa quantità di dati, che, per essere funzionali allo scopo perseguito, devono essere di qualità; di conseguenza, è necessario evitare errori e *bias*, oltre a scongiurare utilizzi impropri o manipolatori[22]. A tale criticità si lega la correlata difficile imputazione della responsabilità giuridica, dal momento che a seconda dei casi può cambiare la partecipazione umana all'azione e alla decisione che conduce a eventuali danni[23].

In merito alla possibilità di errori e *bias*, è paradigmatico il caso di Eric Loomis, in cui è emerso che il software di algoritmi predittivi Compas, utilizzato per valutare il rischio di recidiva e pericolosità sociale, sovrastimava alcuni fattori quali l'appartenenza ad un certo gruppo etnico[24].

Errori e *bias* possono condurre a decisioni illogiche, irrazionali o illegittime, come nei casi giurisprudenziali in ambito nazionale sull'utilizzo di soluzioni di intelligenza artificiale nell'attività

---

[21] Cfr. M. OREFICE, *I big data. Regole e concorrenza*, in *Politica del diritto*, fasc. 4, 2016, p. 706 ss.; G. COLANGELO, *Big data*, piattaforme e antitrust, in *Mercato Concorrenza Regole*, fasc. 3, 2016, p. 426.

[22] Cfr. G. COLANGELO, *op. cit.*, p. 428 ss. Più ampiamente, cfr. C. O' NEIL, *Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, trad. it., Milano, 2017.

[23] Cfr. la risoluzione del Parlamento europeo del 16 febbraio 2017 recante «*raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*» e la comunicazione della Commissione europea «*L'intelligenza artificiale per l'Europa*» COM(2018) 237 *final* del 25 aprile 2018. Al riguardo cfr. C. TREVISI, *La regolamentazione in materia di Intelligenza artificiale, robot, automazione: a che punto siamo*, in *Rivista di diritto dei media*, fasc. 2, 2018, pp. 447-458; M. INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Responsabilità civile e previdenza,* fasc. 5, 2019, p. 1762 ss.

1. [24] La sentenza *State of Wisconsin v. Eric Loomis*, 881 N.W.2d 749 (2016) ha legittimato l'uso del software Compas ritenendo che rispettasse il principio del giusto processo, dal momento che si trattava solo di un ausilio a disposizione del giudice per supportare la sua valutazione e non il motivo esclusivo della decisione; sulla base della natura proprietaria del software, a Loomis non è stato concesso l'accesso al codice sorgente, utile per poter comprendere e contestare le decisioni. Ma gli studi sul software Compas hanno mostrato margini di errore e "imparità" nelle predizioni, a seconda del gruppo etnico di riferimento. Sul caso cfr., *inter alia*, J. LARSON, S. MATTU, L. KIRCHNER, J. ANGWIN, *How we analyzed the COMPAS recidivism algorithm*, in *ProPublica*, 5, 9, 2016; A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal*, fasc. 1, 2019, p. 19; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, fasc. 1, 2019, p. 68; A. SIMONCINI, S. SUWEIS, *op. cit.*, p. 93 ss. Sull'utilizzo di algoritmi e intelligenza artificiale nella giustizia penale G. CONTISSA, G. LASAGNI, G. SARTOR, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Diritto di Internet. Digital Copyright e Data Protection*, fasc. 2, 2019, pp. 619-634.

vincolata delle amministrazioni pubbliche. Le sentenze hanno riguardato l'utilizzo di un sistema informatico, basato su algoritmi, da parte del Ministero dell'Istruzione nell'assegnazione delle sedi nei procedimenti di mobilità dei docenti nella scuola secondaria: l'algoritmo ha condotto a decisioni particolarmente discutibili, che, di conseguenza, sono state contestate dagli interessati e hanno determinato una serie di pronunce, di particolare interesse per i principi in esse espressi[25].

Alcune sentenze, quali TAR Lazio, sez. III bis, 10 settembre 2018, n. 9224, TAR Lazio, sez. III bis, 27 maggio 2019, n. 6606 e TAR Lazio, sez. III bis, 13 settembre 2019, n. 10964, che richiamano *in toto* la prima, si concentrano proprio sul pericolo di errore in cui possono incorrere i sistemi di intelligenza artificiale e, per tale motivo, arrivano ad escludere, anche in casi complessi e ampi da gestire, la possibilità di demandare ad algoritmi l'intera attività amministrativa. L'orientamento è di netta chiusura all'impiego di algoritmi per decisioni amministrative, anche laddove scaturenti da un'attività vincolata, dal momento che non si ritiene sostituibile l'essere umano con algoritmi, che possono solo supportare, costituire un ausilio e avere una funzione servente e mai autonoma nell'attività amministrativa[26].

In tali sentenze l'algoritmo viene ritenuto incapace di assicurare le garanzie procedimentali previste dalla normativa e i principi di trasparenza, partecipazione e obbligo di motivazione con i correlati diritti processuali (diritto di azione e difesa in giudizio), finalizzati all'effettiva realizzazione delle previsioni costituzionali; al riguardo la sentenza TAR Lazio, sez. III bis, 10 settembre 2018, n. 9224 richiama gli artt. 3, 24 e 97 della Costituzione, l'art. 6 della Convenzione europea dei diritti dell'uomo e gli artt. 3, 6, 7, 8, 10 e 10-bis della legge 241/1990. Secondo questo orientamento, infatti, l'algoritmo non permette all'interessato e al giudice di comprendere l'iter logico-giuridico seguito dall'amministrazione per giungere al provvedimento[27].

---

[25] In specifico TAR Lazio, sez. III bis, 22 marzo 2017, n. 3769; TAR Lazio, sez. III bis, 10 settembre 2018, n. 9224; Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270; TAR Lazio, sez. III bis, 27 maggio 2019, n. 6606; TAR Lazio, sez. III bis, 13 settembre 2019, n. 10964. Sulla vicenda rilevano, altresì, le sentenze TAR Lazio, sez. III bis, 21 marzo 2017, n. 3742 e TAR Lazio, sez. III bis, 22 marzo 2017, n. 3769, che si sono occupate dell'accesso al codice sorgente del software dell'algoritmo di gestione della procedura della mobilità dei docenti, qualificandolo quale atto amministrativo informatico e concedendo il relativo accesso. Su tale *corpus* giurisprudenziale e, più ampiamente, sulla decisione automatizzata in ambito amministrativo e sulle problematiche connesse cfr. G. PESCE, *Digital first. Amministrazione digitale: genesi, sviluppi e prospettive*, Napoli, 2018, p. 96 ss.; L. VIOLA, *L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte*, in *Il Foro Amministrativo*, fasc. 9, 2018, p. 1598 ss.; A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, cit., p. 1149 ss.

[26] Cfr. A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., p. 73 ss.

[27] Così TAR Lazio, sez. III bis, 10 settembre 2018, n. 9224, che parla espressamente di «meccanismo informatico o matematico del tutto impersonale e orfano di capacità valutazionali delle singole fattispecie concrete, tipiche invece della tradizionale e garantistica istruttoria procedimentale che deve informare l'attività amministrativa, specie ove sfociante in atti provvedimentali incisivi di posizioni giuridiche soggettive di soggetti privati e di conseguenziali ovvie ricadute anche sugli apparati e gli assetti della pubblica amministrazione». Secondo il TAR non è possibile mortificare e comprimere gli istituti di relazione del privato con i pubblici poteri, quali partecipazione, trasparenza e accesso, «soppiantando l'attività umana con quella impersonale, che poi non è attività, ossia prodotto delle azioni dell'uomo, che può essere svolta in applicazione di regole o procedure informatiche o matematiche».

Di conseguenza, il TAR sostiene che le procedure informatiche, per quanto precise e persino laddove giungano ad essere "perfette", «non possano mai soppiantare, sostituendola davvero appieno, l'attività cognitiva, acquisitiva e di giudizio che solo un'istruttoria affidata ad un funzionario persona fisica è in grado di svolgere» e, pertanto, al fine di assicurare il rispetto delle garanzie procedimentali, il funzionario deve rimanere «il dominus del procedimento stesso», riservando alle procedure informatiche un ruolo meramente strumentale, servente e ausiliario in seno al procedimento amministrativo, che non deve divenire dominante o surrogatorio dell'attività dell'uomo[28].

A tale orientamento, che sostanzialmente nega la possibilità di sostituire l'attività amministrativa umana, anche laddove vincolata, ricorrendo all'utilizzo di algoritmi, si affianca un diverso indirizzo, sposato dal TAR Lazio, sez. III bis, 22 marzo 2017, n. 3769 e dal Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270[29]: secondo tale giurisprudenza l'algoritmo in ambito pubblico è giuridicamente ammissibile e legittimo per attività vincolate prive di discrezionalità, consentendo anzi di raggiungere in modo più efficace i principi dell'attività amministrativa, garantendo minori costi, abbattimento dei tempi e maggior garanzia di imparzialità.

Secondo il TAR Lazio, sez. III bis, 22 marzo 2017, n. 3769 «l'attività vincolata è compatibile con la logica propria dell'elaboratore elettronico in quanto il software traduce gli elementi di fatto e i dati giuridici in linguaggio matematico dando vita a un ragionamento logico formalizzato che porta a una conclusione che, sulla base dei dati iniziali, è immutabile».

Come evidenzia il Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270, l'assenza di intervento umano in un'attività automatica, secondo regole predeterminate elaborate dall'uomo[30], e l'affidamento di tale attività a un efficiente elaboratore elettronico «appaiono come doverose declinazioni dell'art. 97 C. coerenti con l'attuale evoluzione tecnologica».

Tale orientamento, pertanto, ammette e incentiva l'utilizzo di algoritmi per attività amministrative vincolate, ma ne sottopone la legittimità di utilizzo all'esigenza che l'algoritmo soggiaccia ai principi generali dell'attività amministrativa quali trasparenza, pubblicità, ragionevolezza e proporzionalità.

Al fine di utilizzare l'algoritmo nel contesto amministrativo, questo deve essere conoscibile in tutti i suoi aspetti, comprensibile e soggetto alla cognizione, al pieno sindacato e alla valutazione della legittimità della decisione e della correlata correttezza del processo informatico in tutte le sue componenti da parte

[28] TAR Lazio, sez. III bis, 10 settembre 2018, n. 9224.

[29] Si tratta della sentenza del Consiglio di Stato a seguito della pronuncia del TAR Lazio del 1° dicembre 2016, n. 12026, che aveva rigettato il ricorso. Sulla sentenza cfr., *inter alia*, S. CRISCI, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici" (commento di Consiglio di Stato, Sezione VI, sentenza 8 aprile 2019, n. 2270)*, in *Diritto di Internet. Digital Copyright e Data Protection*, fasc. 2, 2019, p. 377 ss.; M. MANCARELLA, *Algoritmo e atto amministrativo informatico: le basi nel CAD*, in *Diritto di Internet. Digital Copyright e Data Protection*, fasc. 3, 2019, pp. 469-476.

[30] In tali casi la discrezionalità va individuata nel momento dell'elaborazione dello strumento tecnologico.

del giudice, che deve poter accertare nel processo automatizzato il rispetto dei principi, delle finalità e delle norme previste dalla legge o dalla stessa amministrazione.

Emerge anche per quanto riguarda l'algoritmo, così come per l'azione delle amministrazioni pubbliche svolta dai funzionari, l'esigenza di conformità ai principi fondamentali dell'attività amministrativa; la sindacabilità in merito all'esercizio del potere si configura quale declinazione diretta del diritto alla difesa dell'interessato. Secondo il Consiglio di Stato, l'utilizzo di procedure "robotizzate" non può essere motivo di elusione dei principi dell'ordinamento. La regola tecnica che governa l'algoritmo resta una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi soltanto applicata da questa[31]; tale regola algoritmica assume piena valenza giuridica e amministrativa, ma come tale deve rispettare i principi dell'ordinamento.

Alla luce di tali considerazioni, nella fattispecie oggetto di giudizio il Consiglio di Stato ha ravvisato l'impossibilità di comprendere le modalità con cui, attraverso l'algoritmo, sono stati assegnati i posti disponibili. In tal caso, infatti, gli esiti sono risultati connotati da illogicità e irrazionalità, essendosi verificate situazioni paradossali, in contrasto con le disposizioni di riferimento. Questo aspetto ha costituito un vizio tale da inficiare la procedura per violazione dei principi di imparzialità, pubblicità e trasparenza.

Dall'analisi di tali sentenze emerge la necessità che l'intelligenza artificiale rispetti i valori e i principi dell'ordinamento, tra cui dignità, libertà, pieno sviluppo della persona, eguaglianza e non discriminazione e, in caso di impiego nel contesto pubblico, buon andamento dell'amministrazione fondato su imparzialità, trasparenza, pubblicità, economicità ed efficacia: la conformità a tali principi può risultare non sempre agevole laddove l'azione e la conseguente decisione siano algoritmicamente determinate, basandosi su inferenze e correlazioni. A ben vedere, le problematiche giuridiche sono legate strettamente alle caratteristiche tecniche che connotano le soluzioni di intelligenza artificiale.

Alla necessità di garantire il rispetto di valori etici e principi giuridici da parte dell'intelligenza artificiale si collega un altro aspetto particolarmente delicato e significativo.

Il governo di dati e algoritmi, anima dell'intelligenza artificiale, conferisce un enorme potere e una correlata responsabilità, soprattutto in caso di utilizzi spregiudicati, manipolatori o discriminatori, potendo provocare una conseguente asimmetria di potere tra chi li controlla e gli utenti. Nell'utilizzo di tali soluzioni si affaccia il pericolo di impiegare in vario modo la conoscenza e le previsioni, anche per profilazioni incuranti dei diritti e delle libertà degli individui e per finalità diverse da quelle originarie con potenziali effetti discriminatori, che possono condurre fino a forme di sorveglianza e di controllo, ancor

[31] Al riguardo A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, cit., p. 1149 ss. evidenzia l'intenzione del Consiglio di Stato di salvare l'aspetto della volontà umana nel momento della costruzione della regola algoritmica.

più pericolose laddove scaturenti dall'interazione tra soggetti pubblici e privati.

Da ciò consegue, nell'utilizzo dell'intelligenza artificiale, la necessità di una valutazione sull'impatto giuridico, sociale ed etico di tali soluzioni, al fine di prevenire i potenziali effetti negativi sulla dignità umana, sulle libertà e sui diritti fondamentali[32].

A tale valutazione si accompagnano complessi interrogativi cui gli ordinamenti odierni si trovano di fronte, come l'individuazione dei valori etici e giuridici con i quali educare e istruire i sistemi di intelligenza artificiale e, congiuntamente, l'individuazione di principi comuni tra ordinamenti diversi[33]: a tali criticità si lega la complessa valutazione relativa all'introduzione o all'adattamento di categorie giuridiche e norme. Questi profili richiamano gli aspetti evidenziati nella storia del rapporto tra diritto e tecnologie informatiche, relativi all'esigenza di *governance* e alla vocazione necessariamente sovranazionale dei problemi.

Il rispetto dei valori etici della società e dei correlati principi di diritto si traduce, altresì, nella necessaria tutela da offrire ai diversi diritti in gioco, che esige l'osservanza delle norme di riferimento. Al riguardo rilevano in modo significativo la tutela della persona e la protezione dei dati personali, profili che caratterizzano il rapporto tra diritto e tecnologia fin dal suo avvento e che emergono anche in relazione all'intelligenza artificiale.

Nel caso dell'intelligenza artificiale, di norma si tratterà di insiemi di dati misti, fattispecie prevista dal regolamento europeo 2018/1807 sulla circolazione dei dati non personali e dalla comunicazione della Commissione europea «*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*» del 29 maggio 2019[34].

In presenza di insiemi di dati misti, nei casi in cui i dati personali e i dati non personali siano indissolubilmente legati, il regolamento (UE) 2018/1807 lascia impregiudicata l'applicazione del regolamento (UE) 2016/679[35], che si applica pienamente all'insieme di dati misti, anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme dei dati[36]. Nei casi in cui, invece, dati

[32] Cfr. «*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*», adottate il 23 gennaio 2017 dal Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale.

[33] Cfr. A. D'ALOIA, *op. cit.*, pp. 3-31.

[34] Le linee guida sono state adottate ai sensi dell'art. 8, par. 3, reg. (UE) 2018/1807, che impone alla Commissione europea di pubblicare orientamenti sull'interazione tra i due regolamenti europei «in particolare per quanto concerne gli insiemi di dati composti sia da dati personali che da dati non personali».

[35] Art. 2, par. 2, reg. (UE) 2018/1807. Il concetto di "indissolubilmente legati" non è definito dai regolamenti, ma può essere ravvisato nelle situazioni in cui separare dati personali e dati non personali sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile.

[36] Comunicazione della Commissione europea «*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*» del 29 maggio 2019. Sull'interazione tra regolamento (UE) 2018/1807 e regolamento (UE) 2016/679 cfr. M.L. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato concorrenza regole*, fasc. 2, 2019, pp. 293-313.

personali e dati non personali non siano indissolubilmente legati, il regolamento (UE) 2018/1807 si applica alla parte dell'insieme contenente i dati non personali e, parallelamente, il regolamento (UE) 2016/679 si applica alla parte dell'insieme contenente i dati personali.

Pertanto, nel caso dell'intelligenza artificiale, che per lo più si basa su *big data* e, quindi, su insiemi di dati misti, di norma si applicherà la normativa in materia di *data protection*[37].

Al riguardo, però, emergono molteplici ed eterogenee problematiche.

Le caratteristiche tecniche dell'intelligenza artificiale e i suoi elementi fondanti (dati e algoritmi) mostrano criticità ontologiche nel rispetto della disciplina in materia di protezione dei dati personali, di cui al regolamento (UE) 2016/679, teso ad una protezione effettiva ed efficace dell'individuo: in particolare, tali caratteristiche rischiano di scontrarsi apertamente con alcuni principi fondamentali della disciplina, finalizzati a garantire il rispetto della persona e della sua libertà di autodeterminazione.

L'intelligenza artificiale si basa su elaborazioni e inferenze e su processi di natura deterministica distanti dal ragionamento umano, capaci di condurre anche a risultati diversi e inaspettati, e ha bisogno di un'enorme mole eterogenea di dati per condurre a risultati significativi: una maggiore quantità di dati, infatti, rende maggiormente accurate le relazioni tra gli stessi[38]. Di conseguenza, nel caso dell'intelligenza artificiale può risultare complesso il rispetto del principio di limitazione della finalità, che prevede la raccolta dei dati personali per finalità determinate, esplicite e legittime e il successivo trattamento in modo che non sia incompatibile con tali finalità[39]. Il volume dei dati, la varietà delle fonti e il modo di operare degli algoritmi rendono, inoltre, difficile il rispetto del criterio di minimizzazione dei dati e dei relativi principi di adeguatezza, pertinenza e limitazione dei dati personali a quanto necessario rispetto alle finalità del trattamento[40] e rischiano di inficiare la qualità, l'esattezza e l'accuratezza dei dati[41].

Pertanto, i principi cardine della disciplina in materia di *data protection*, costituiti da limitazione della finalità, esattezza e minimizzazione dei dati, rischiano di essere depotenziati in tale contesto.

Inoltre, nelle caratteristiche di funzionamento dell'intelligenza artificiale emergono criticità profonde che rischiano di minare i fondamenti della disciplina europea.

Il concetto di "dato personale", su cui si basa anche la dicotomia tra i regolamenti europei, può risultare insufficiente, dal momento che i dati afferenti a gruppi o comunità, appartenenti quindi a più persone, i

[37] Il rispetto della disciplina in materia di *data protection* è necessario a garantire fiducia da parte degli utenti nell'intelligenza artificiale; cfr. la comunicazione della Commissione europea «*Piano coordinato sull'intelligenza artificiale*» COM(2018) 795 *final* del 7 dicembre 2018: «Per una maggiore fiducia, necessaria affinché la società accetti e usi l'IA, la tecnologia dovrebbe essere prevedibile, responsabile, verificabile, dovrebbe rispettare i diritti fondamentali e seguire regole etiche».

[38] Cfr. A. MANTELERO, *op. cit.*, pp. 135-144; V. MAYER-SCHÖNBERGER, K. CUKIER, *op. cit.*, p. 42; G. SARTOR, M. VIOLA DE AZEVEDO CUNHA, *op. cit.*, pp. 657-680.

[39] Art. 5, par. 1, lett. b), reg. (UE) 2016/679.

[40] Art. 5, par. 1, lett. c), reg. (UE) 2016/679.

[41] Art. 5, par. 1, lett. d), reg. (UE) 2016/679.

metadati e i dati inferiti, possono risultare estremamente significativi[42]. Gli stessi dati anonimi possono non rimanere tali e le tecniche di anonimizzazione possono sollevare criticità; il pericolo sta nelle inferenze che possono essere tratte: ogni dato può finire per essere identificativo e quindi personale, soprattutto nelle correlazioni tra moltitudini di dati diversi[43].

In relazione all'intelligenza artificiale vacilla anche il paradigma basato sulla trasparenza, sull'informativa e sul consenso: proprio per le esaminate caratteristiche distintive, è dubbio che in tale contesto le informazioni rese siano capaci di fornire effettiva conoscenza sul funzionamento degli algoritmi, sull'impatto e sulle conseguenze sulla persona e che, di conseguenza, il consenso possa considerarsi libero[44].

Nel caso dell'intelligenza artificiale rileva particolarmente la disposizione dedicata al «processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione», di cui all'art. 22 del regolamento (UE) 2016/679, che attribuisce all'interessato «il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». Ma la norma non si applica al verificarsi di alcune ampie condizioni, in particolare «nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato».

Nel caso del consenso esplicito e in quello di necessità per la conclusione o l'esecuzione del contratto, il titolare del trattamento è comunque tenuto ad attuare «misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[45]. Pertanto, esiste quanto meno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione, ma nuovamente emergono le difficoltà scaturenti dalle caratteristiche tecniche dell'intelligenza artificiale, in particolare la logica inferenziale e deterministica, che può rendere difficile comprendere le decisioni e, di conseguenza, contestarle.

Le complesse ed eterogenee problematiche etiche e giuridiche sollevate dall'intelligenza artificiale determinano l'esigenza di una *governance* sovranazionale, esigenza intercettata, a livello internazionale, dal

[42] Cfr. C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Bologna, 2015, p. 28 ss.
[43] Cfr. G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, p. 34 ss.
[44] Artt. 7, 12-14, reg. (UE) 2016/679. Cfr. F.H. CATE, V. MAYER-SCHÖNBERGER, *Notice and consent in a world of Big Data*, in *International Data Privacy Law*, 2013, vol. 3, n. 2, pp. 67-73.
[45] Art. 22, par. 3, reg. (UE) 2016/679.

Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nelle «*Guidelines on artificial intelligence and data protection*» del 25 gennaio 2019 e, a livello europeo, dalla Commissione europea con la comunicazione «*L'intelligenza artificiale per l'Europa*» COM(2018) 238 *final* del 25 aprile 2018, con il «*Piano coordinato sull'intelligenza artificiale*» COM(2018) 795 *final* del 7 dicembre 2018 e con il *White Paper* «*On Artificial Intelligence - A European approach to excellence and trust*» COM(2020) 65 *final* del 19 febbraio 2020[46].

Alla costruzione di una *governance* sovranazionale, sono finalizzate, altresì, la Dichiarazione di cooperazione sull'intelligenza artificiale, firmata da 25 Stati membri il 10 aprile 2018, cui hanno aderito in seguito anche altri Stati, e la *European AI Alliance*, piattaforma partecipativa dedicata alla discussione relativa allo sviluppo e all'impatto dell'intelligenza artificiale.

Lo sforzo europeo di governare l'intelligenza artificiale, riuscendo a tutelare i singoli e la collettività, ha preso forma anche nella nomina da parte della Commissione europea di un Gruppo di esperti ad alto livello sull'intelligenza artificiale, che ha fornito orientamenti etici per un'intelligenza artificiale affidabile con un lavoro presentato l'8 aprile 2019 come «*Ethics guidelines for trustworthy AI*»[47]. Le linee guida delineano un'intelligenza artificiale meritevole di fiducia o affidabile, che per essere tale deve rispettare le norme e la legalità, osservare i principi etici e mostrare robustezza. A tali fini, l'"IA affidabile" deve rispondere e deve essere valutata sulla base di quattro principi etici (rispetto dell'autonomia umana; prevenzione dei danni; equità; esplicabilità) e di sette requisiti fondamentali (intervento e sorveglianza umani; robustezza tecnica e sicurezza; riservatezza e *governance* dei dati; trasparenza; diversità, non discriminazione ed equità; benessere sociale ed ambientale; *accountability*)[48].

Alla luce dell'analisi svolta, nel caso dell'intelligenza artificiale emergono prepotentemente quegli aspetti che caratterizzano la storia del rapporto tra diritto e tecnica, quali la tutela della persona rispetto alla tecnologia, la necessità di *governance* e l'esigenza di un approccio sovranazionale, che si traducono nel bisogno di un'evoluzione della regolazione giuridica, in modo da rendere la tecnologia conforme ai principi e alle norme di riferimento, costruendo un nuovo rapporto tra diritto e tecnica[49].

[46] Rileva, altresì, la risoluzione del Parlamento europeo del 16 febbraio 2017 recante «*raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*».

[47] Il lavoro, reso pubblico il 18 dicembre 2018 in una prima versione, a seguito di consultazione pubblica è stato presentato nella versione finale l'8 aprile 2019.

[48] A livello nazionale, sotto il profilo strategico rilevano il Libro Bianco «*L'intelligenza artificiale al servizio del cittadino*», curato dall'Agenzia per l'Italia Digitale (AgID) e dalla Task Force sull'Intelligenza artificiale, pubblicato nel marzo 2018, e le «*Proposte per una strategia italiana per l'intelligenza artificiale*», elaborate dal Gruppo di Esperti sull'intelligenza artificiale del Ministero dello Sviluppo Economico, pubblicate nel luglio 2019.

[49] Il paragrafo 3 del presente saggio è dedicato a tali aspetti.

2.2. *Blockchain*

Allo scopo di approfondire il rapporto che lega diritto e tecnica e, di conseguenza, esaminare la correlata necessaria evoluzione della regolazione giuridica, accanto all'intelligenza artificiale, è particolarmente significativa un'altra tecnologia emergente, la *blockchain*[50].

Come nel caso dell'intelligenza artificiale, anche l'analisi giuridica della *blockchain* deve partire dall'oggetto della regolazione e, pertanto, dalle caratteristiche tecniche: l'esame della tecnologia *blockchain* è necessario perché proprio in alcuni connotati distintivi emergono criticità per il diritto, i diritti e le norme esistenti.

La *blockchain* è una *species* del *genus* delle *distributed ledger technologies* (DLT), ossia tecnologie di registro distribuito e disintermediato *peer-to-peer*, in cui le voci del *database* sono replicate in una serie di nodi e la regolazione avviene mediante meccanismi di consenso condiviso; le DLT si distinguono dalle architetture centralizzate *client-server*, basate invece sul controllo di un'autorità di gestione.

In specifico la *blockchain* consiste in una "catena di blocchi": i dati, inseriti per mezzo di crittografia asimmetrica, sono allocati in blocchi, accompagnati da *hash* e validazione temporale, concatenati tra loro attraverso il richiamo dell'*hash* del blocco precedente in quello successivo[51]; questo aspetto determina la caratteristica dell'immutabilità unilaterale[52]. Ogni nuovo blocco è validato da alcuni nodi (cosiddetti *miners*) per mezzo della risoluzione di un problema matematico complesso, che vale una ricompensa; tale meccanismo incentiva la corretta validazione dei blocchi[53]. Le transazioni sono validate con il consenso della maggioranza degli utenti.

La *blockchain*, in modo immutabile, conserva la memoria storica delle transazioni e, in modo distribuito e paritetico, garantisce a ciascun partecipante una copia di ciascuna operazione: in tal modo sono garantite sicurezza e resistenza rispetto a potenziali attacchi[54]. Tali caratteristiche rendono la tecnologia *blockchain* assimilabile a un registro o a un libro mastro digitale, che non necessita di un intermediario o di un

---

[50] La presente analisi su *blockchain* e *smart contract* muove dalle riflessioni contenute in F. FAINI, Blockchain *e diritto. La "catena del valore" tra documenti informatici,* smart contracts *e* data protection, in *Responsabilità civile e previdenza*, fasc. 1, 2020, pp. 297-316.

[51] Dato che ogni *hash* contiene l'*hash* del blocco precedente, il tentativo di modificare un blocco comporterebbe la modifica di tutti quelli successivi, determinando una "rottura" della catena. In considerazione del meccanismo di funzionamento, la rettifica dei dati è difficilmente esercitabile: è possibile realizzarla solo con la creazione di un nuovo ulteriore blocco che riporti la rettifica dei dati inseriti e validati.

[52] L'immodificabilità deve essere intesa da un punto di vista unilaterale (un singolo da solo non può modificare i dati), ma non è una caratteristica valida in assoluto: laddove si pervenisse a un controllo sulla maggioranza del consenso la modifica diventerebbe possibile. Cfr. A. PALLADINO, *L'equilibrio perduto della blockchain tra* platform revolution *e* GDPR compliance, in *Rivista di diritto dei media*, fasc. 2, 2019, p. 152 ss.

[53] Cfr. M. GIULIANO, *op. cit.*, p. 989 ss.; L. PAROLA, P. MERATI, G. GAVOTTI, Blockchain *e* smart contract*: questioni giuridiche aperte*, in *I Contratti*, fasc. 6, 2018, p. 681; A. GAMBINO, C. BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Il diritto dell'informazione e dell'informatica*, fasc. 3, 2019, p. 619 ss.; P.P. PIRANI, *Gli strumenti della finanza disintermediata:* Initial Coin Offering *e* blockchain, in *Analisi Giuridica dell'Economia*, fasc. 1, 2019, p. 329 ss.; G. LEMME, *Gli* smart contracts *e le tre leggi della robotica*, in *Analisi Giuridica dell'Economia*, fasc. 1, 2019, p. 129 ss.

[54] Cfr. A. WRIGHT, P. DE FILIPPI, *op. cit.*, pp. 1-58.

soggetto terzo certificatore[55] ed è applicabile proficuamente in molteplici settori in ambito privato e pubblico[56].

Pertanto, volendo individuare i tratti distintivi, le caratteristiche principali della *blockchain* sono costituite da disintermediazione, decentralizzazione, distribuzione e vocazione transnazionale; immutabilità, inalterabilità e persistenza dei dati; meccanismo distribuito *peer-to-peer* di consenso, fiducia e incentivazione[57]; trasparenza, tracciabilità e sicurezza; funzioni di *hash*, validazione temporale e crittografia asimmetrica[58].

Tali caratteristiche si declinano in maniera parzialmente diversa nelle differenti tipologie di *blockchain*: le *blockchains permissionless* o *unpermissioned* o pubbiche si distinguono per essere aperte e liberamente accessibili da chiunque senza autorizzazioni (es. Bitcoin ed Ethereum[59]); le *blockchains permissioned* o private sono chiuse e non accessibili pubblicamente, dal momento che le autorizzazioni sono gestite da un'autorità centrale[60]; le *blockchains ibride*, dette altresì consorzi, sono parzialmente decentrate, dal momento che esiste un controllo sul meccanismo di consenso da parte di alcuni nodi preselezionati, che hanno maggiore influenza degli altri.

Nel caso della *blockchain*, come in quello dell'intelligenza artificiale, rilevano i profili che da sempre

---

[55] Al riguardo, come sottolinea A. GAMBINO, *Vizi e virtù del diritto computazionale*, in *Il diritto dell'informazione e dell'informatica*, fasc. 6, 2019, p. 1169 ss. «la *blockchain* permette di ottenere la fiducia e l'affidabilità che nel passato erano necessariamente legate ad una figura terza, un notaio o un pubblico ufficiale».

[56] Sono eterogenei gli ambiti di applicazione della *blockchain*: il settore finanziario e monetario, la pubblica amministrazione, i processi aziendali, la *supply chain*, il settore agroalimentare, il settore assicurativo, l'identità digitale, la gestione dei diritti di proprietà intellettuale, i brevetti, il settore energetico, il patrimonio culturale e artistico, la proprietà di *assets*, etc.

[57] I meccanismi di consenso sono diversi: *Proof of Work* (utilizzato da Bitcoin), *Proof of Stake*, etc., per una rassegna dei quali si rinvia a F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, p. 26 ss.; A. CONTALDO, F. CAMPARA, *Blockchain, cripto valute, smart contract, industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie*, Pisa, 2019, p. 12 ss.

[58] Si tratta di un sistema a doppia chiave pubblica e privata: la chiave privata è conosciuta e utilizzata dal soggetto titolare per cifrare i dati e la chiave pubblica è utilizzata dal destinatario per decifrare i dati e verificare l'utente (ciò non consente la diretta riferibilità all'identità del soggetto, in particolare nelle *permissionless*); le due chiavi sono correlate e indipendenti.

[59] Bitcoin è la prima applicazione pratica della tecnologia *blockchain*, impiegata per la creazione di una moneta elettronica basata su un protocollo decentralizzato *peer-to-peer*, il cui inventore è riconosciuto in Satoshi Nakamoto (pseudonimo sotto cui si cela la misteriosa identità dell'inventore); cfr. S. NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, in *bitcoin.org*, 2008. Ethereum è un protocollo con lo scopo principale di fornire una piattaforma *open source* per incentivare lo sviluppo di applicazioni decentralizzate (*decentralized applications* – DApps), come gli *smart contracts*. L'inventore di Ethereum è Vitalik Buterin; cfr. V. BUTERIN, *Ethereum White Paper. A next generation smart contract & decentralized application platform*, in *https://ethereum.org*, 2013, pp. 1-37. Al riguardo cfr. M. FAIOLI, E. PETRILLI, D. FAIOLI, Blockchain*, contratti e lavoro. La ri-rivoluzione del digitale nel mondo produttivo e nella PA*, in *Economia & lavoro*, fasc. 2, 2016, p. 145 ss.

[60] La distinzione tra *blockchains* pubbliche e private fa riferimento alla gestione dell'infrastruttura informatica: le pubbliche non sono gestite da nessuno, le private invece sono gestite da una persona, da un'organizzazione o da un gruppo di individui. Cfr. M. GIULIANO, *op. cit.*, p. 989 ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 21 ss.; A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss. Secondo A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss. gli aspetti principali di differenza tra *blockchains permissionless* e *permissioned* consistono nei seguenti: identificabilità dei soggetti; modalità di selezione dei nodi e grandezza della rete; meccanismo di consenso condiviso; trasparenza del contenuto dei blocchi.

caratterizzano il rapporto tra diritto e tecnologia, evidenziati ripercorrendone brevemente la storia: da un lato emerge l'esigenza di *governance* collegata alla necessità di un approccio sovranazionale, dall'altro prende forma lo scontro ontologico tra le caratteristiche tecniche e il rispetto di principi e norme del diritto, in tal caso esacerbato dalla logica orizzontale e dal meccanismo distribuito *peer-to-peer* di consenso e fiducia, che mal si concilia con il sistema di tutele basato sulla centralizzazione e sul controllo, e acutizzato, altresì, da problemi di coordinamento delle norme nazionali con le norme europee.

Sotto il profilo dell'esigenza di *governance* e di un approccio non limitato ai confini nazionali, rilevano particolarmente gli atti di riferimento europei, che si occupano proprio di costruire una *governance* sovranazionale della *blockchain*.

Il Parlamento europeo, nella risoluzione del 3 ottobre 2018 sulle tecnologie di registro distribuito e *blockchain*, pone attenzione alle tecnologie in oggetto, capaci di creare fiducia attraverso la disintermediazione e di «migliorare l'efficienza dei costi delle transazioni eliminando intermediari e costi di intermediazione, oltre ad aumentare la trasparenza delle transazioni, ridisegnando anche le catene del valore e migliorando l'efficienza organizzativa attraverso un decentramento affidabile». Secondo il Parlamento europeo, il paradigma informatico delle *distributed ledger technologies*, grazie ai meccanismi di cifratura e controllo, «può democratizzare i dati e rafforzare la fiducia e la trasparenza, fornendo un percorso sicuro ed efficace per l'esecuzione delle transazioni», rafforzando l'autonomia dei cittadini.

Il Parlamento europeo è consapevole della necessità di *governance*, anche alla luce del fatto che i pericoli e i problemi sottesi all'utilizzo di tali tecnologie non sono ancora completamente noti: le *distributed ledger technologies*, quali tecnologie in continua evoluzione, necessitano di «un quadro favorevole all'innovazione che consenta e incoraggi la certezza del diritto e rispetti il principio della neutralità tecnologica, promuovendo nel contempo la protezione dei consumatori, degli investitori e dell'ambiente, aumentando il valore sociale della tecnologia, riducendo il divario digitale e migliorando le competenze digitali dei cittadini».

Di conseguenza, l'Unione europea si è impegnata nella costruzione di una *governance* sovranazionale della *blockchain*, attraverso l'istituzione dell'*EU Blockchain Observatory and Forum* il 1° febbraio 2018, cui è attribuita la funzione di raccogliere informazioni, mappare le principali iniziative esistenti, monitorare gli sviluppi e analizzare le tendenze, esaminare il potenziale socio-economico e affrontare le sfide, cercando di garantire un approccio uniforme e comune a livello europeo[61], e l'istituzione dell'*European Blockchain*

[61] L'*EU Blockchain Observatory and Forum*, istituito da parte della Commissione europea, ha, a sua volta, formato due gruppi di lavoro: il *Blockchain Policy and Framework Conditions Working Group*, deputato a definire le condizioni politiche, legali e regolamentari necessarie per la diffusione su larga scala delle applicazioni basate sulla *blockchain* e designato ad esaminare questioni quali gli *smart contracts* e la protezione dei dati personali, e l'*Use Cases and Transition Scenarios Working Group*, chiamato a concentrarsi sui casi di utilizzo più promettenti, con particolare attenzione alle applicazioni del settore pubblico come identità e servizi, assistenza sanitaria, energia e rendicontazione ambientale. Sono particolarmente

Partnership il 10 aprile 2018, che mira a consolidare il ruolo dell'Europa nello sviluppo e nella diffusione della tecnologia *blockchain* per mezzo di un approccio uniforme a livello europeo[62]: i rappresentanti dei Paesi partecipanti lavorano sinergicamente, al fine di stabilire le linee di intervento utili per sfruttare il potenziale dei servizi basati sulla *blockchain* a beneficio dei cittadini, della società e dell'economia. Nel quadro di queste iniziative, il partenariato coopera per la creazione dell'*European Blockchain Services Infrastructure* (EBSI), capace di supportare la fornitura di servizi pubblici transfrontalieri nell'Unione europea, utilizzando la tecnologia *blockchain* e garantendo alti standard di sicurezza e protezione dei dati personali[63].

Sotto il profilo del rapporto tra tecnica e diritto e del correlato rispetto da parte di tale tecnologia emergente di principi, norme e diritti, al fine di analizzare i problemi che emergono, acutizzati dalla logica orizzontale, dalla disintermediazione e dal meccanismo distribuito *peer-to-peer*, rileva il fatto che il legislatore nazionale sia intervenuto in materia, generando peraltro alcuni problemi di coordinamento con le norme europee.

L'art. 8-ter del d.l. 135/2018 convertito in legge 12/2019, infatti, definisce le tecnologie basate su registri distribuiti e gli *smart contracts* conferendo specifici effetti giuridici e demandando la regolazione tecnica a standard e linee guida di competenza dell'Agenzia per l'Italia digitale (AgID)[64].

La definizione delle "tecnologie basate su registri distribuiti" (*distributed ledger technologies*), tra le quali rientra la *blockchain*, riprende le caratteristiche tecniche esaminate: le *distributed ledger technologies* sono «*le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili*»[65].

La definizione, esplicitamente limitata alle *distributed ledger technologies*, è stata oggetto di critiche per il fatto

interessanti i *reports* tematici prodotti dall'Osservatorio, che affrontano anche le sfide giuridiche poste da tale tecnologia, disponibili al link *https://www.eublockchainforum.eu/eu-blockchain-observatory-forum*.

62 Cfr. *https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership*.

63 L'*European Blockchain Services Infrastructure* (EBSI) prenderà forma come una rete di nodi distribuiti in tutta l'Unione europea; cfr. *https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi*.

64 Il legislatore non ha scelto di integrare il d.lgs. 82/2005, ossia il Codice dell'amministrazione digitale, ma ha lasciato la norma formalmente fuori dal Codice, seppur per ambito di materia e per i contenuti trattati potesse ambire a farne parte, in considerazione del fatto che il d.lgs. 82/2005 dovrebbe porsi quale riferimento principale in tema di innovazione tecnologica. Sull'analisi della norma cfr. C. BOMPREZZI, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto, mercato, tecnologia*, 2019, pp. 1-7; F. SARZANA DI S. IPPOLITO, Blockchain *e* smart contract *nel nuovo decreto semplificazioni*, in *Diritto di Internet. Digital Copyright e Data Protection*, fasc. 1, 2019, pp. 17-23. A livello nazionale, sotto il profilo strategico è stato nominato dal Ministero dello Sviluppo Economico nel dicembre 2018 un Gruppo di Esperti per l'elaborazione di una strategia nazionale in materia di tecnologie basate su registri distribuiti e *blockchain*.

65 Art. 8-ter, comma 1, d.l. 135/2018 convertito in legge 12/2019.

che rischia di confondere le *distributed ledger technologies* e le *blockchains*: alcune caratteristiche, infatti, connotano più propriamente queste ultime, in particolare nella tipologia *permissionless* (inalterabilità, immodificabilità e verificabilità dei dati da parte di ciascun partecipante). Di conseguenza, rischia di determinarsi una sovrapposizione erronea tra i due fenomeni, che in realtà differiscono: la *blockchain* è una particolare tipologia, una *species* del *genus* delle *distributed ledger technologies*, dotata di propri tratti distintivi[66].

Secondo quanto previsto dalla disposizione nazionale, la memorizzazione di un documento informatico attraverso l'uso di *distributed ledger technologies* produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41 del regolamento (UE) n. 910/2014; ai fini della produzione di tali effetti le tecnologie basate su registri distribuiti devono possedere gli standard tecnici individuati dall'AgID[67].

Tale profilo solleva criticità nel coordinamento tra la disposizione nazionale e la normativa europea. L'art. 41 del regolamento (UE) eIDAS n. 910/2014, infatti, prevede gli effetti giuridici sia della validazione temporale semplice sia della validazione temporale qualificata, che differiscono da un punto di vista giuridico, dal momento che per avere la presunzione di accuratezza della data e dell'ora e di integrità dei dati ai quali data e ora sono associate, è necessaria la validazione temporale elettronica qualificata[68], mentre nel caso della validazione temporale elettronica semplice, la valutazione è rimessa al libero apprezzamento del giudice[69].

Alla luce del rinvio generico della disposizione italiana all'art. 41 del regolamento (UE) eIDAS n. 910/2014, non è chiaro a quale validazione temporale elettronica, qualificata o meno, intenda riferirsi il legislatore nel caso della memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti, aspetto rilevante in considerazione del diverso valore della validazione temporale elettronica semplice e qualificata.

Al riguardo la norma rinvia agli standard tecnici individuati dall'AgID, che le tecnologie basate su registri distribuiti devono possedere ai fini della produzione di tali effetti[70]: gli standard dell'AgID potrebbero contribuire a sciogliere il nodo interpretativo, anche se al momento tale rinvio rischia di aggravare le

---

66 Cfr. C. BOMPREZZI, *op. cit.*, p. 2; F. SARZANA DI S. IPPOLITO, *op. cit.*, p. 18.

67 Art. 8-ter, commi 3 e 4, d.l. 135/2018 convertito in legge 12/2019.

68 Art. 41, par. 2, reg. (UE) eIDAS n. 910/2014. La validazione temporale elettronica qualificata è definita dall'art. 3, par. 1, n. 34 e i requisiti sono previsti nell'art. 42 del reg. (UE) eIDAS n. 910/2014. Al riguardo rileva il considerando 62 del reg. (UE) eIDAS, ai sensi del quale «*al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il* […] *regolamento dovrebbe richiedere l'uso di un sigillo elettronico avanzato o di una firma elettronica avanzata o di altri metodi equivalenti*»: ai sensi del considerando, infatti, è «*prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal sigillo elettronico avanzato o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti*»

69 La definizione di validazione temporale elettronica semplice è contenuta nell'art. 3, par. 1, n. 33, reg. (UE) eIDAS n. 910/2014.

70 Art. 8-ter, commi 3 e 4, d.l. 135/2018 convertito in legge 12/2019.

problematiche in gioco.

In merito, infatti, il regolamento (UE) eIDAS n. 910/2014 pone il principio di non discriminazione, previsto dal primo paragrafo dell'art. 41, secondo cui «*alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata*»[71].

Dal momento che la disposizione italiana prevede che le *distributed ledger technologies* debbano possedere gli standard di AgID ai fini della produzione degli effetti, si può ipotizzare che il legislatore intenda riferirsi alla validazione temporale elettronica qualificata, dal momento che il riferimento a quella semplice verrebbe a limitare quanto previsto a livello europeo dal principio di non discriminazione. Nel caso di interpretazione come validazione temporale elettronica qualificata, gli standard di AgID devono essere interpretati in modo restrittivo e possono costituire soltanto un ausilio e un mezzo per misurare il rispetto dei requisiti di cui all'art. 42 del regolamento (UE) eIDAS, non potendo certo sostituirsi agli stessi, ponendosi altrimenti in contrasto con la disciplina europea, che peraltro, in quanto contenuta in un regolamento europeo, prevale sulle norme nazionali in contrasto, disapplicandole[72].

Al fine di fugare dubbi interpretativi e problematiche applicative, garantendo coerenza tra la norma italiana e il quadro di regolazione europea, sotto tale profilo sarà opportuno esaminare la regolazione tecnica costituita dagli standard di AgID che, anche se costituiscono *soft law*, potranno contribuire a dare contenuto ai principi posti dalla norma e a un maggior coordinamento tra la norma italiana e la disciplina europea.

Oltre ai problemi di coordinamento tra norme nazionali ed europee, il rapporto tra *blockchain* e diritto è caratterizzato dallo scontro tra alcune caratteristiche tecniche e le norme a tutela di diritti, tra tecnologia e diritto positivo. Al riguardo, come nel caso dell'intelligenza artificiale, la criticità più significativa è costituita dalla tutela della persona rispetto alla tecnologia e, in specifico, dal rispetto della disciplina in materia di protezione dei dati personali di cui al regolamento (UE) 2016/679 e al d.lgs. 196/2003 modificato dal d.lgs. 101/2018[73].

Sotto il profilo della *data protection*, le caratteristiche tecniche distintive della *blockchain*, punti di forza di tale tecnologia, rischiano di trasformarsi in punti di debolezza, capaci di creare criticità nel rispetto dei

[71] Il principio di non discriminazione vale anche per i documenti elettronici, le firme elettroniche, i sigilli elettronici e i servizi elettronici di recapito certificato; artt. 25, 35, 43 e 46, reg. (UE) eIDAS n. 910/2014.

[72] Cfr. C. BOMPREZZI, *op. cit.*, p. 6.

[73] Sulla difficile interazione tra *blockchain* e *data protection* cfr., *inter alia*, M. BERBERICH, M. STEINER, *Blockchain Technology and the GDPR-How to Reconcile Privacy and Distributed Ledgers?*, in *European Data Protection Law Review*, fasc. 2, 2016, pp. 422-426; L. MOEREL, *Blockchain & Data Protection…and Why They Are Not on a Collision Course*, in *European Review of Private Law*, fasc. 6, 2019, pp. 825-852.

principi e delle norme previste[74].

Nelle tecnologie *blockchain* la funzione di *hash* può essere qualificata come un'operazione di pseudonimizzazione, che come tale comporta l'applicazione della normativa in materia di protezione dei dati personali[75].

La pseudonimizzazione indica il trattamento che avviene in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile[76]. A differenza dell'anonimizzazione, i dati restano personali a seguito della pseudonimizzazione, che costituisce una misura di sicurezza al fine di proteggere i dati oggetto di trattamento: la persona fisica è identificabile, dal momento che i dati non sono direttamente riconducibili alla persona, ma possono diventarlo con l'utilizzo di informazioni aggiuntive[77].

Di conseguenza, in caso di utilizzo della *blockchain* è necessario il rispetto dei principi applicabili al trattamento dei dati personali previsti dal regolamento europeo 2016/679, in specifico dall'art. 5, tra i quali rilevano la minimizzazione dei dati[78] e la limitazione della conservazione[79]. La difficoltà sta nel fatto che la *blockchain* per il suo funzionamento replica i dati nei vari nodi, scontrandosi così con il principio di minimizzazione, e conserva i dati in modo perpetuo, confliggendo in tal modo con il principio della limitazione della conservazione.

Le caratteristiche della *blockchain* determinano ulteriori complesse problematiche in materia di protezione dei dati personali.

La disciplina in tema di *data protection* individua alcune figure di riferimento, fondamentali ai fini della *governance* e dell'applicazione normativa: accanto all'interessato, ossia la persona fisica identificata o identificabile, cui i dati personali si riferiscono[80], il titolare, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, che, singolarmente o insieme ad altri titolari, determina le finalità e i mezzi del trattamento di dati personali, e il responsabile, ossia la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo eventualmente preposto dal titolare che tratta dati personali per

74 Cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.; A. PALLADINO, *op. cit.*, p. 153 ss.
75 In tal senso si esprime anche il Parlamento europeo nella risoluzione del 3 ottobre 2018.
76 Art. 4, par. 1, n. 5, reg. (UE) 2016/679.
77 Cfr. G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista trimestrale di diritto e procedura civile*, fasc. 2, 2018, p. 441 ss.; A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.; M. GIULIANO, *op. cit.*, p. 989 ss.
78 Art. 5, par. 1, lett. c), reg. (UE) 2016/679, secondo cui i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
79 Art. 5, par. 1, lett. e), reg. (UE) 2016/679, secondo cui i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
80 Art. 4, par. 1, n. 1, reg. (UE) 2016/679.

suo conto[81]. Il regolamento europeo 2016/679 prevede la possibilità della contitolarità del trattamento, nel caso in cui due o più titolari del trattamento determinino congiuntamente le finalità e i mezzi del trattamento[82].

L'individuazione di queste figure è determinante per l'attuazione della disciplina, dal momento che a tali soggetti si applicano obblighi a tutela della persona e dei suoi dati, come il principio fondamentale di responsabilizzazione, secondo cui il titolare è competente per il rispetto dei principi e deve essere in grado di comprovarlo[83].

Sotto il profilo soggettivo, rileva la specifica tipologia di *blockchain*: nelle *permissioned* è individuabile il titolare nel soggetto che governa l'infrastruttura e nel caso dei consorzi si può fare leva sulla contitolarità del trattamento, ma nelle *permissionless* diventa complesso individuare tali figure, a causa delle caratteristiche di disintermediazione e distribuzione.

In tal caso sono state ipotizzate diverse ricostruzioni, che spaziano da chi decreta in tali casi l'assenza di titolari, con il conseguente problema di applicazione della disciplina[84], a chi qualifica tutti i nodi come contitolari o responsabili o, ancora, titolari per sé e responsabili per gli altri[85]. In tale ipotesi, però, risulta difficile individuare la determinazione "congiunta" delle finalità e dei mezzi del trattamento posta come condizione normativa necessaria a qualificare i soggetti come contitolari[86]: si determina una conseguente difficoltosa individuazione pratica degli stessi e una correlata problematica distribuzione di responsabilità che rischia di compromettere l'efficacia della tutela[87]. Anche nella variante interpretativa che li prevede quali responsabili, questi lo sarebbero *de facto*, mancando il previsto atto di designazione da parte del titolare[88].

Un'altra interpretazione, invece, individua il titolare nello sviluppatore del software, ma anche questa posizione non convince perché in concreto tale soggetto può limitarsi a fornire la soluzione senza determinare finalità e mezzi del trattamento; in alcuni casi può elaborare dati per conto di un altro soggetto e atteggiarsi quale responsabile[89].

Non mancano problemi anche per quanto riguarda l'esercizio dei diritti dell'interessato, rafforzati dal

81 Art. 4, par. 1, nn. 7 e 8, reg. (UE) 2016/679.
82 Art. 26, reg. (UE) 2016/679.
83 Art. 5, par. 2, reg. (UE) 2016/679. Il titolare è tenuto a garantire *accountability* e sicurezza, ai sensi degli artt. 24 e 32, reg. (UE) 2016/679, dal momento che deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento; il regolamento europeo, negli artt. 82-84, prevede responsabilità e sanzioni utili a garantire effettività alle previsioni.
84 Cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.; M. GIULIANO, *op. cit.*, p. 989 ss.
85 In tal senso W. MAXWELL, J. SALMON, *A guide to blockchain and data protection*, Brussels, 2017, p. 11; M. FINK, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, fasc. 4, 2018, p. 17 ss.
86 Art. 26, reg. (UE) 2016/679.
87 Cfr. A. PALLADINO, *op. cit.*, p. 153 ss.
88 Cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.
89 Cfr. M. GIULIANO, *op. cit.*, p. 989 ss.

regolamento europeo 2016/679, quali il diritto all'accesso a dati e informazioni (art. 15), il diritto di rettifica e integrazione (art. 16), il diritto alla cancellazione (diritto all'oblio) (art. 17), il diritto di limitazione di trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), il diritto di opposizione al trattamento (art. 21) e il diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (art. 22). La difficoltà di individuazione del titolare, infatti, rischia di impedire l'effettivo esercizio dei diritti da parte dell'interessato[90].

Inoltre, in considerazione delle caratteristiche di immodificabilità, inalterabilità e persistenza dei dati, in relazione alla tecnologia *blockchain* non risultano esercitabili i diritti di rettifica[91], limitazione e cancellazione dei dati stessi da parte dell'interessato, dal momento che tali diritti risultano sostanzialmente inattuabili a fronte delle specifiche caratteristiche tecniche della *blockchain*[92]. Peraltro in questa tecnologia il procedimento porta alle conseguenze tramite automatismi: di conseguenza, può non risultare agevole neppure il rispetto del diritto a non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato o, almeno, del diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione[93].

Infine, la vocazione transnazionale della *blockchain*, unita alla pseudonimizzazione, rende difficile stabilire il luogo del trattamento e la distribuzione dei nodi può allargarsi fuori dall'ambito territoriale europeo: emergono difficoltà concrete nell'applicazione della disciplina, che si estende anche fuori dai confini dell'Unione europea[94], e prendono vita dubbi in merito all'applicazione delle norme relative al trasferimento dei dati all'estero, prevista dal regolamento (UE) 2016/679[95].

Le criticità giuridiche esaminate derivano direttamente dalle caratteristiche tecniche distintive della *blockchain*; più ampiamente, l'approccio concettuale del regolamento europeo in materia di *data protection*, che prevede un trattamento centralizzato dei dati personali fondato sul controllo e sulla responsabilizzazione, risulta faticosamente adattabile a una tecnologia che si caratterizza invece proprio

[90] Cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.

[91] In tal senso M. FINK, *op. cit.*, p. 21 ss.

[92] Cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.; M. GIULIANO, *op. cit.*, p. 989 ss. Secondo A. PALLADINO, *op. cit.*, p. 155 ss., riguardo ai diritti che prevedono aggiornamento, rettifica e integrazione, mantenendo la conservazione dei dati, la *blockchain* non osta necessariamente, dal momento che è possibile validare un nuovo blocco di dati contenente l'aggiornamento, la rettifica e l'integrazione operate dall'interessato, mentre i diritti che prevedono una demolizione del dato (quali cancellazione e limitazione di trattamento) risultano tendenzialmente inconciliabili con tale tecnologia che si basa sull'immodificabilità dei dati stessi.

[93] Si tratta di quanto previsto dall' art. 22, reg. (UE) 2016/679.

[94] L'art. 3, par. 2, reg. (UE) 2016/679 prevede l'applicazione del regolamento «*al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione*».

[95] Cfr. A. PALLADINO, *op. cit.*, p. 153 ss.; M. GIULIANO, *op. cit.*, p. 989 ss.

per decentralizzazione, disintermediazione e distribuzione[96].

2.3. *Smart contract*

Il difficile rapporto tra tecnologia e diritto nel caso della *blockchain* è ancor più apprezzabile in una sua significativa applicazione, lo *smart contract*, che per le sue caratteristiche tecniche distintive genera una serie di problematiche giuridiche nel garantire il rispetto dei principi e delle norme, anche in tal caso acutizzate da difficoltà di coordinamento tra le specifiche disposizioni nazionali e il quadro giuridico di riferimento[97]. Come per l'intelligenza artificiale e la *blockchain*, l'analisi giuridica deve muovere dall'esame delle caratteristiche tecniche.

Nello *smart contract*[98], nel momento in cui sono soddisfatte le condizioni contrattuali tradotte dal codice informatico nel linguaggio macchina, si attivano automaticamente gli effetti conseguenti con le caratteristiche tipiche della *blockchain*, in particolare l'immutabilità e l'irreversibilità: gli effetti contrattuali si eseguono automaticamente al verificarsi delle condizioni predeterminate dalle parti e descritte sotto forma di codice informatico secondo la logica "*if this then that*"[99]: si determina così un meccanismo di *self-enforcement* delle regole, potendosi scorgere un'evoluzione dei contratti automatici, tipologia contrattuale usata per il distributore automatico di bevande o la *vending machine*[100].

L'affidamento al codice informatico piuttosto che all'adempimento delle parti genera vantaggi significativi, che consistono nell'eliminazione del rischio di inadempimento, del ricorso a intermediari e

---

[96] Cfr. M. FINK, *op. cit.*, p. 17 ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 68 ss.

[97] Lo *smart contract* non è indissolubilmente legato da un punto di vista identitario alla tecnologia *blockchain* per concretizzarsi, ma può basarsi anche su un diverso sistema informatico automatizzato, che ottenga la fiducia delle parti e a cui le stesse rimettano l'esecuzione dell'accordo che hanno negoziato precedentemente; cfr. C. BOMPREZZI, *op. cit.*, p. 3; A. DAVOLA, R. PARDOLESI, Smart contract*: lusinghe ed equivoci dell'innovazione purchessia*, in *Il Foro italiano,* fasc. 4, 2019, p. 195 ss.; G. LEMME, *op. cit.*, p. 147 ss.

[98] Nick Szabo è considerato l'ideatore dello *smart contract*; cfr. N. SZABO, *Smart contracts: building blocks for digital markets*, in *EXTROPY: The Journal of Transhumanist Thought*, 16, 18, 1996, p. 2 ss.; N. SZABO, *The idea of Smart Contracts*, in *Nick Szabo's Papers and Concise Tutorials*, 6, 1997; N. SZABO, *Formalizing and Securing Relationships on Public Networks*, in *First Monday*, vol. 2, n. 9, 1997. Sugli *smart contracts* cfr., *inter alia*, P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *La Nuova giurisprudenza civile commentata*, fasc. 1, 2017, pp. 107-119; E. MIK, *Smart Contracts: Terminology, Technical Limitations and Real World Complexity*, in *Law, Innovation and Technology*, vol. 9, n. 2, 2017, pp. 269-300; I. BASHIR, *Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained*, II ed., Birmingham, 2018; S. COMELLINI, M. VASAPPOLO, *Blockchain, Criptovalute, I.C.O. e Smart Contract*, Santarcangelo di Romagna, 2019; R. DE CARIA, *The Legal Meaning of Smart Contracts*, in *European Review of Private Law*, fasc. 6, 2019, pp. 731-752; F. DELFINI, *Blockchain, Smart Contracts e innovazione tecnologica: l'informatica e il diritto dei contratti*, in *Rivista di diritto privato*, fasc. 2, 2019, pp. 167-178; A. GAMBINO, A. STAZI, D. MULA, *Diritto dell'informazione e dell'informatica*, III ed., Torino, 2019, p. 182 ss.; A. STAZI, *Automazione contrattuale e "contratti intelligenti". Gli* smart contracts *nel diritto comparato*, Torino, 2019.

[99] Il determinarsi degli effetti può dipendere da elementi interni al codice (es. una data, un termine, etc.) o da circostanze esterne; in tale ultimo caso interviene una fonte di informazione esterna, un "oracolo", che permette di verificare se siano soddisfatte le clausole previste (es. le condizioni atmosferiche, l'avvenuta consegna di un bene, l'orario di un mezzo di trasporto, etc.). Cfr. L. PAROLA, P. MERATI, G. GAVOTTI, *op. cit.*, p. 683 ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 94 ss.

[100] Cfr. A. DAVOLA, R. PARDOLESI, *op. cit.*, p. 195 ss. Al riguardo, cfr. A. CICU, *Gli automi nel diritto privato*, in *Il Filangeri*, n. 8, 1901, p. 561 ss.

dei relativi costi in termini economici e di tempo, rendendo più sicura la relazione contrattuale ed evitando l'insorgere di controversie[101]: nel corso dell'analisi emergerà, però, come si tratti di vantaggi potenziali, suscettibili di sfumare nella realtà a fronte di esigenze concrete da perseguire, che determinano la necessità della presenza di quegli elementi che in teoria gli *smart contracts* permettono di superare.

Il nostro ordinamento definisce lo "*smart contract*" nel secondo comma dell'art. 8-ter del d.l. 135/2018 convertito in legge 12/2019 come «*un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse*»; lo *smart contract* soddisfa il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'AgID con linee guida: la qualificazione normativa oscilla tra software e documento informatico[102].

Al riguardo emergono complesse problematiche nel rispetto dei principi e delle norme esistenti, proprio a causa del funzionamento dello *smart contract* e delle sue caratteristiche tecniche.

La definizione di *smart contract* della norma italiana, che fa riferimento all'esecuzione capace di "vincolare" automaticamente due o più parti sulla base di effetti predefiniti dalle stesse, determina una controversa problematica circa l'inquadramento, la natura e la qualificazione giuridica degli *smart contracts*, scaturente direttamente dal rapporto che lega l'accordo giuridico e il codice informatico.

La prima ricostruzione individua negli *smart contracts* veri e propri accordi negoziali, capaci di sostituirsi completamente ai contratti tradizionali e di concretizzare una diversa modalità di manifestazione del consenso, formazione e conclusione dell'accordo[103]: il codice informatico costituirebbe il vero e proprio accordo, nel quale si esprime la volontà contrattuale, con forza di legge tra le parti ai sensi dell'art. 1372 c.c., dotato della capacità di essere automaticamente eseguito[104].

Un diverso orientamento, invece, qualifica gli *smart contracts* come meri strumenti idonei a gestire gli accordi e a eseguire una volontà espressa altrove in un precedente accordo contrattuale, capaci di garantire l'automazione dell'adempimento e l'esecuzione automatica: in tale ricostruzione, pertanto, i "contratti intelligenti" si collocano nel momento dell'adempimento e nella fase esecutiva dell'accordo[105]. Lo *smart contract* non riguarderebbe la fase di formazione del contratto, che rimarrebbe costituita dall'accordo delle parti, esterno o *off-chain*, ma la fase dell'adempimento contrattuale, che avverrebbe in modo automatico

[101] P. CUCCURU, *op. cit.*, p. 111 ss.

[102] La definizione rischia di limitare lo *smart contract* all'ambito contrattuale: lo *smart contract* sicuramente può avere forma di contratto, ma può altresì prestarsi ad altre funzioni; in tal senso C. BOMPREZZI, *op. cit.*, p. 3 ss.

[103] Cfr. M. GIULIANO, *op. cit.*, p. 989 ss.

[104] Al riguardo c'è chi parla di negozi giuridici per *facta concludentia*; cfr. D. DI SABATO, *Smart contracts: robot che gestiscono il rischio contrattuale*, in *Contratto e impresa*, fasc. 2, 2017, pp. 378-402.

[105] Cfr. L. PAROLA, P. MERATI, G. GAVOTTI, *op. cit.*, p. 685 ss.; G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 441 ss.; S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Il Foro Amministrativo*, fasc. 10, 2018, pp. 1787-1816.

al verificarsi delle condizioni espresse nel codice informatico: anche in considerazione della difficile traduzione in codice informatico delle clausole negoziali[106], tale orientamento mira a inquadrare più agevolmente gli *smart contracts* nell'ordinamento giuridico, preservando la volontà delle parti.

L'inquadramento dello *smart contract* nell'una o nell'altra ricostruzione dipende strettamente dalla specifica fattispecie, ossia da quale delle due ipotesi lo *smart contract* realizzi in concreto e, correlativamente, dal rapporto tra accordo e codice informatico[107]: la definizione contenuta nella norma italiana, seppur con qualche ambiguità lessicale, nel fare diretto riferimento all'esecuzione, parrebbe alludere alla seconda ricostruzione[108].

Oltre alla qualificazione giuridica e all'inquadramento dei "contratti intelligenti", emergono ulteriori rilevanti problematiche giuridiche, scaturenti dal coordinamento degli *smart contracts* con la disciplina di riferimento: l'equiparazione a contratti veri e propri, ma anche l'interpretazione che li confina alla fase dell'adempimento pongono, infatti, conseguenti criticità nel garantire in tali fattispecie il rispetto di quanto previsto dalla normativa civilistica[109].

Il fatto che lo *smart contract* configuri un documento informatico, infatti, comporta il necessario rispetto delle norme europee e nazionali di riferimento, ossia quanto previsto dal regolamento (UE) eIDAS n. 910/2014, dal codice civile, dal d.lgs. 82/2005 (Codice dell'amministrazione digitale) e dalle relative regole tecniche. Sotto tale profilo, però, si scorgono difficoltà a conciliare la *lex cryptographia* degli *smart contracts* con le regole poste dal diritto positivo[110].

Una problematica, in particolare laddove lo *smart contract* esprima la volontà contrattuale, è individuabile nell'identificazione delle parti contraenti, proprio alla luce del meccanismo di funzionamento della *blockchain* che si basa sulla pseudonimizzazione dei soggetti; in considerazione dei requisiti che caratterizzano giuridicamente il contratto, è necessario che le parti siano identificate, anche se in ogni caso permane il rischio che il soggetto non sia chi afferma di essere, dal momento che non ci sono mezzi

106 Cfr. A. DAVOLA, R. PARDOLESI, *op. cit.*, pp. 195-207.

107 M. GIULIANO, *op. cit.*, p. 989 ss. evidenzia l'importanza della ricostruzione della fattispecie concreta per valutare se la volontà delle parti si esprima attraverso lo *smart contract* oppure l'accordo sia *off-chain* e lo *smart contract* si limiti ad eseguire l'accordo avvenuto altrove.

108 In particolare risulta ambiguo il termine "vincolare" usato nella definizione, che pare alludere al fatto che le parti si obbligano, a meno di non interpretare il verbo come collegato alla caratteristica di immutabilità della *blockchain* e alla conseguente impossibilità di inadempimento; cfr. C. BOMPREZZI, *op. cit.*, p. 3 ss., che sottolinea l'inadeguatezza del termine, dal momento che il programma per elaboratore dovrebbe agire a supporto delle parti contraenti più che vincolarle.

109 Cfr. G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, cit., pp. 441-460.

110 Cfr. G. LEMME, *op. cit.*, p. 148, che evidenzia come «il processo di divaricazione piena tra *civil law* (ma tutto sommato anche *common law*) e *lex cryptographia* si stia oramai ineluttabilmente compiendo».

per testarne la capacità di agire, con il conseguente rischio di annullabilità del contratto[111].

La norma italiana, infatti, pone l'accento sulla previa identificazione informatica delle parti: lo *smart contract* soddisfa il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'AgID con linee guida[112].

Al riguardo, ai fini della riconducibilità del documento informatico al soggetto[113], lo *smart contract* può essere ascritto al processo di cui all'art. 20, comma 1-bis, del d.lgs. 82/2005[114], ossia può qualificarsi come "firma elettronica avanzata identificata", che è ravvisabile laddove il documento informatico sia formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dalle linee guida dell'AgID con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore[115].

Laddove risulti perseguibile tale qualificazione, lo *smart contract*, sotto il profilo del valore giuridico, soddisferebbe il requisito della forma scritta per gli atti di cui all'art. 1350, numero 13, del codice civile (ossia gli atti previsti dalla legge, esclusi quelli indicati dal n. 1 al n. 12 della disposizione) e, sotto il profilo probatorio, avrebbe l'efficacia prevista dall'art. 2702 del codice civile: la "firma elettronica avanzata identificata", quale *species* della firma avanzata, infatti, possiede il relativo valore giuridico e probatorio del *genus* cui appartiene[116].

Questa interpretazione si attaglia alle *blockchains permissioned*, dove i partecipanti sono previamente identificati, ma può non essere adeguata alle *blockchains permissionless*. In tal caso, laddove, a causa dell'assenza dei requisiti normativi necessari, non possa essere riconosciuto il valore di firma avanzata, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il valore probatorio saranno rimessi alla libera valutazione del giudice, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità, ai sensi dell'art. 20, comma 1-bis, d.lgs. 82/2005[117].

Di conseguenza, la norma italiana solleva tale significativo aspetto critico afferente all'idoneità ad

---

111 Cfr. A. STAZI, *op. cit.*, p. 143 ss. Al riguardo, secondo M. GIACCAGLIA, *Considerazioni su* Blockchain *e* smart contracts *(oltre le criptovalute)*, in *Contratto e impresa*, fasc. 3, 2019, p. 962 tali problematiche appartengono più ampiamente alla disciplina dei contratti telematici e non solo alla tecnologia *blockchain*.

112 Art. 8-ter, comma 2, d.l. 135/2018 convertito in legge 12/2019.

113 I dati registrati nella *blockchain* possono qualificarsi come documento informatico alla luce della normativa di riferimento, mentre più problematica può risultare proprio l'attribuzione del documento informatico al soggetto che lo ha creato; cfr. M. GIULIANO, *op. cit.*, p. 989 ss.

114 Tale processo è stato introdotto nel Codice dell'amministrazione digitale dal d.lgs. 217/2017.

115 Cfr. G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 441 ss.; C. BOMPREZZI, *op. cit.*, pp. 4-5.

116 L'ordinamento giuridico italiano prevede un sistema graduale di firme elettroniche, idoneo ad attribuire diverso valore giuridico e diversa efficacia probatoria al documento informatico a cui sono apposte: firma elettronica cosiddetta semplice, elettronica avanzata, elettronica qualificata (disciplinate dal regolamento europeo eIDAS) e digitale (prevista e disciplinata dal d.lgs. 82/2005); sia consentito il rinvio a F. FAINI, *Documenti e contratti nella società tecnologica*, in F. FAINI, S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche*, Torino, 2017, pp. 111-148.

117 Cfr. C. BOMPREZZI, *op. cit.*, p. 5; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 51 ss.

assolvere il requisito della forma scritta, che può mutare a seconda della tipologia di *blockchain* impiegata e che, anche in tal caso, scaturisce strettamente dalle caratteristiche tecniche concrete: il valore giuridico e l'efficacia probatoria sono diversi in conformità alla differente capacità tecnologica di garantire sicurezza e affidabilità circa l'identità dei soggetti e l'integrità dei dati.

Un'altra rilevante criticità dei "contratti intelligenti", scaturente dalle caratteristiche tecniche, riguarda l'applicazione delle disposizioni in materia di inadempimento: nello *smart contract* l'adempimento è automatico e prescinde dal comportamento delle parti, impossibilitate a tenere comportamenti scorretti e a violare l'accordo[118].

Tale aspetto può essere interpretato come un vantaggio degli *smart contracts*, che tecnologicamente eliminano il rischio dell'inadempimento delle parti, il ricorso a intermediari e l'insorgere di controversie, contribuendo a garantire certezza del diritto; però non mancano giuridicamente problemi di coordinamento con la normativa civilistica. Al riguardo, inoltre, rileva l'art. 1375 c.c. ai sensi del quale l'esecuzione del contratto deve avvenire secondo buona fede: ciò non significa sempre un'esecuzione letterale dell'accordo, come avviene invece nel caso dell'esecuzione automatica, ma può doversi declinare in una valutazione qualitativa.

In merito una significativa questione aperta dagli *smart contracts*, soprattutto laddove equiparati ad accordi negoziali, afferisce al tema dell'interpretazione del contratto e alle norme degli artt. 1362-1371 c.c., che "secondo buona fede" portano a dover cercare "la comune intenzione delle parti" e che non riuscirebbero a trovare applicazione, dal momento che il codice informatico eseguirà in modo rigido quanto programmato senza elasticità e margini di interpretazione[119].

Proprio le stringhe di codice informatico che danno vita e forma agli *smart contracts* generano significative problematiche sotto la lente giuridica nella fase di predisposizione del contratto, in quella di attuazione dello stesso e nel caso di insorgenza di problematiche.

Nel momento della predisposizione del contratto, infatti, può risultare particolarmente complesso tradurre matematicamente in linguaggio algoritmico clausole generali e principi interpretabili (buona fede, correttezza, ragionevolezza, diligenza, giusta causa, etc.), in quanto elementi non misurabili e, pertanto, di difficile traduzione informatica.

Nella fase dell'attuazione, gli *smart contracts*, comprensibili a chi conosce il linguaggio di programmazione, possono determinare una sorta di barriera semantica e destare problemi di comprensione e intelligibilità

[118] Cfr. S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, cit., pp. 1787-1816; G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 441 ss., che non vede particolari difficoltà, dal momento che l'adempimento, laddove si tratti di pagamento, è atto dovuto; secondo l'Autrice maggiori problemi emergono in caso di alternativa tra due obbligazioni, dal momento che la scelta relativa sarebbe automatica sfuggendo alla volontà, oppure in caso di revoca della dichiarazione contrattuale che tecnicamente potrebbe essere inattuabile (mancherebbe il tempo di revoca).

[119] Cfr. L. PAROLA, P. MERATI, G. GAVOTTI, *op. cit.*, p. 685 ss.; F. SARZANA DI S. IPPOLITO, *op. cit.*, p. 22.

del contenuto non solo per le stesse parti (forse superabili facendo riferimento ai principi di autoresponsabilità e affidamento), ma anche per un eventuale giudice, che avrà bisogno di un "interprete" per conoscerne il contenuto[120].

Infine, la difficile trasposizione in linguaggio macchina delle clausole contrattuali determina anche la possibilità concreta che si verifichino divergenze tra l'accordo (e la correlata volontà delle parti) e la traduzione nell'algoritmo, generando possibili conseguenti vizi. Questo aspetto evidenzia la necessità di solide competenze trasversali di natura giuridica e informatica per riuscire a tradurre le condizioni giuridiche in codice informatico e pone in luce il pericolo dell'eccessiva semplificazione di clausole complesse richiesta dal linguaggio di programmazione, con il connesso rischio di risultati indesiderati o erronei[121]. A tale profilo si affianca il pericolo di problematiche di ordine meramente tecnico, come nel caso in cui il codice subisca una modifica spontanea nel corso dell'esecuzione, influendo sugli effetti[122].

Sotto tali profili, il vantaggio della tecnologia *blockchain* consistente nell'eliminazione di intermediari viene sostanzialmente annullato dal fatto che è necessario comunque avvalersi di un terzo cui riporre fiducia, un soggetto con competenze informatiche, che, come esaminato, risulterà cruciale nella fase di predisposizione del contratto, ma potrà servire anche al momento dell'attuazione o in caso di problematiche: di conseguenza, si assiste più propriamente a un mutamento della tipologia di intermediario, che in tal caso è chiamato a svolgere la funzione tecnica di tradurre in linguaggio informatico l'accordo, invece che quella giuridica di seguirne la genesi, la vita e l'esecuzione[123]. Al riguardo, inoltre, come emerge dall'analisi, è discutibile che l'automatismo renda evitabile il ricorso a figure terze a livello giuridico, proprio alla luce delle problematiche che solleva: tale considerazione determina che in questi casi siano necessarie diverse figure di intermediari, dotate di competenze informatiche e giuridiche, chiamate a collaborare in modo sinergico al fine di garantire risultati scevri da criticità ed errori.

Nel caso degli *smart contracts* risulta critica anche l'applicazione degli strumenti relativi alla fase patologica del negozio, quali i vizi del consenso (errore, violenza e dolo), che permettono al contraente di chiedere l'annullamento del contratto secondo le norme previste; parimenti possono risultare problematiche l'applicazione degli istituti di nullità e annullamento, la risoluzione del contratto, l'attivazione di rimedi in autotutela o l'inibizione dell'esecuzione a seguito di un provvedimento giudiziale[124]. Tali strumenti sono

120 Cfr. P. CUCCURU, *op. cit.*, p. 113 ss.; G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 441 ss.; M. GIULIANO, *op. cit.*, p. 989 ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 100 ss.; A. STAZI, *op. cit.*, p. 156 ss.

121 In tal senso S. CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, cit., pp. 1787-1816; M.L. PERUGINI, Distributed Ledger Technologies *e sistemi di* blockchain. *Digital currency, smart contract e altre applicazioni*, Vicalvi, 2018, p. 214 ss.

122 Cfr. A. STAZI, *op. cit.*, p. 167 ss.

123 In senso analogo P. CUCCURU, *op. cit.*, p. 113 ss.; M. GIACCAGLIA, *op. cit.*, p. 958 ss.

124 Cfr. L. PAROLA, P. MERATI, G. GAVOTTI, *op. cit.*, p. 686 ss.; M. GIULIANO, *op. cit.*, p. 989 ss.; A. STAZI, *op. cit.*, p. 176 ss. Secondo M.L. PERUGINI, *op. cit.*, p. 214 l'esecuzione automatica degli *smart contracts* mantiene inalterata

predisposti dal diritto al fine di porre legittimo rimedio a patologie del negozio giuridico o a tutelare la parte debole del rapporto, interessi meritevoli di tutela per l'ordinamento, che in tali casi subirebbero un'inevitabile compressione: di conseguenza, le caratteristiche tecnologiche degli *smart contracts* generano un problema di governabilità e controllabilità degli stessi, potendo comportare il sacrificio di esigenze tutelate dal diritto positivo[125].

Alla luce dell'analisi svolta, le problematiche giuridiche esaminate derivano direttamente dalle caratteristiche tecniche distintive della *blockchain* e degli *smart contracts*, quali disintermediazione, decentralizzazione e immutabilità, che devono faticosamente essere coordinate con un sistema di tutele fondato, invece, sulla centralizzazione, sul controllo e sulla presenza di soggetti cui imputare scelte e responsabilità[126].

3. L'evoluzione della regolazione giuridica: il diritto nella tecnica

Le tecnologie emergenti esaminate, intelligenza artificiale, *blockchain* e *smart contract*, evidenziano il complesso rapporto tra diritto e tecnica e la correlata necessità di un'evoluzione della regolazione giuridica.

Una direzione efficace per regolare le tecnologie emergenti può essere individuata proprio nella relazione che lega diritto e tecnica, norme giuridiche e codice informatico; il diritto può avvalersi della tecnica per garantire il suo rispetto: ciò è possibile per mezzo dell'incorporazione di principi, norme e rimedi nella tecnologia, ossia costruendo un "diritto nella tecnica"[127].

Questa strada non è nuova, dal momento che il diritto se ne serve da tempo per regolare la tecnologia: è il caso delle misure tecnologiche di protezione per tutelare il diritto d'autore in caso di opere digitali, in modo che alcune operazioni, come accessi, utilizzi o copie non autorizzate, non solo siano giuridicamente illecite, ma siano anche inibite tecnicamente; la condotta non autorizzata diventa impossibile e la normativa protegge giuridicamente il titolare contro l'elusione delle misure tecnologiche di protezione[128].

L'incorporazione del diritto nella tecnica, in considerazione delle esaminate caratteristiche che connotano le tecnologie emergenti, può costituire una direzione idonea a garantire efficacia ed effettività ai principi e alle norme.

---

la possibilità di intervenire a correzione di eventuali patologie: l'irreversibilità informatica viene bilanciata dal sistema di rivalse e istanze giudiziarie del sistema civilistico, in caso di invalidità o malfunzionamento.

[125] Su tali aspetti cfr. P. CUCCURU, *op. cit.*, p. 113 ss.; M. GIACCAGLIA, *op. cit.*, pp. 961-962.

[126] Cfr. L. PAROLA, P. MERATI, G. GAVOTTI, *op. cit.*, p. 688; M. GIULIANO, *op. cit.*, p. 989 ss., che sottolinea come le norme siano pensate per un paradigma socio-economico in cui vi è sempre un soggetto che gestisce, controlla e che, di conseguenza, è responsabile, a cui imputare gli atti.

[127] Nel senso dell'incorporazione nelle regole informatiche di valori giuridici condivisi anche E. MAESTRI, *op. cit.*, p. 173 ss.

[128] Art. 102-quater, legge 633/1941.

Nel caso dell'intelligenza artificiale, infatti, l'utilizzo di algoritmi deve avvenire nel rispetto dei principi etici e giuridici che informano la normativa di riferimento a tutela di diritti, come la *data protection*, e in ambito pubblico, come evidenziato anche dalla giurisprudenza amministrativa esaminata, nel rispetto dei criteri che guidano l'azione pubblica in materia di procedimento amministrativo, amministrazione digitale, trasparenza e accesso.

Per poter efficacemente governare l'intelligenza artificiale, i profili etici e giuridici devono essere implementati preventivamente a livello tecnologico, al fine di scongiurare o quantomeno minimizzare danni successivi e conseguenti responsabilità, anche in considerazione della difficile individuazione delle stesse. Etica e diritto possono avvalersi della tecnologia per assicurare la loro osservanza e garantire la tutela della persona, del cittadino, della collettività: la tecnologia può agire quale "antidoto" preventivo a possibili violazioni delle norme.

Un modello di "diritto nella tecnica" è insito, del resto, nell'approccio proattivo e preventivo presente nella disciplina europea in materia di protezione dei dati personali, che tutela la persona fin dalla progettazione, per impostazione predefinita e per mezzo della valutazione d'impatto[129]: si tratta dei principi *data protection by design* e *by default*[130], cui si affianca il *data protection impact assessment*[131], nei quali il diritto si avvale della tecnologia per garantire la tutela della dignità e dello sviluppo della persona. Tali principi innovativi del regolamento europeo 2016/679 mirano a una ponderazione preventiva dell'impatto e dei rischi sulla *data protection*, accompagnata dalla responsabilizzazione del titolare del trattamento[132].

---

[129] Cfr. C. FOCARELLI, *op. cit.*, p. 63; A. MANTELERO, *op. cit.*, p. 159 ss.

[130] Il principio *data protection by design*, di cui all'art. 25, par. 1, reg. (UE) 2016/679, prevede che, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare debba mettere in atto «*misure tecniche e organizzative adeguate, quali la pseudonimizzazione*» (di cui all'art. 4, comma 1, n. 5), «*volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati*». A tale criterio si lega il principio *data protection by default*, posto nel secondo paragrafo dell'art. 25, reg. (UE) 2016/679: il titolare deve mettere in atto «*misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento*». L'individuo è tutelato in modo rafforzato dal momento che la norma impedisce l'accesso ai dati personali a un numero indefinito di persone fisiche da parte di macchine (senza l'intervento della persona fisica) e prevede che l'obbligo sia calibrato su aspetti quali la quantità di dati, la portata del trattamento, il periodo di conservazione e l'accessibilità.

[131] Il *Data Protection Impact Assessment* (DPIA) è previsto dall'art. 35 del reg. (UE) 2016/679: quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare effettua, prima di procedere al trattamento, «*una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali*». Tale valutazione deve contenere almeno i requisiti prescritti dalla norma ed è prevista nelle ipotesi poste dalla normativa, tra le quali rientrano i trattamenti automatizzati, come le operazioni di profilazione degli utenti, che permettono una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente sulle persone fisiche.

[132] Cfr. G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove leggi civili commentate*, 2017, fasc. 1, pp. 1-18; L. GRECO, A. MANTELERO, *Industria 4.0, robotica e* privacy-by-design, in *Il diritto dell'informazione e*

Questa logica può essere interpretata estensivamente come approccio idoneo a consentire più ampiamente il rispetto dei principi etici e giuridici di riferimento nell'utilizzo dell'intelligenza artificiale: la tecnologia può assumere una connotazione etica e giuridica *by default* e *by design*[133].

In tal senso si esprime anche l'Unione europea che pone tra i principi fondamentali dell'intelligenza artificiale "*made in Europe*" proprio l'etica "fin dalla progettazione", a cui deve accompagnarsi il principio di "sicurezza fin dalla progettazione"[134].

L'incorporazione del diritto nella tecnica risulta soluzione proficuamente perseguibile anche nel caso della *blockchain* e degli *smart contracts*, al fine di rispettare le norme di riferimento e la tutela di diritti come la protezione dei dati personali.

Sotto tale profilo, nella constatazione che le problematiche si atteggiano diversamente in caso di *blockchains permissioned* o *permissionless*, dove sono più evidenti, al fine di superare le criticità esaminate, la strada è individuabile nell'approccio preventivo, proattivo e tecnico, previsto dallo stesso regolamento (UE) 2016/679, facendo leva anche in tal caso sull'incorporazione dei principi e delle norme nella tecnologia e facendo assolvere al diritto la sua funzione preventiva: la regolazione giuridica può servirsi della tecnologia, svolgendo un'azione preventiva sul *design* dell'architettura tecnologica, adattandola e adeguando alcune caratteristiche distintive della *blockchain*, quali disintermediazione e immutabilità, al fine di perseguire i principi della protezione dei dati personali[135].

In particolare andrebbero immaginate soluzioni in grado di conciliare la tecnologia con i principi della *data protection*, quali la memorizzazione dei dati personali *off-chain* (fuori dalla catena di blocchi), memorizzando sulla stessa un mero riferimento, al fine di garantire l'esercizio dei diritti dell'interessato,

---

dell'informatica, fasc. 6, 2018, p. 875 ss., che sottolineano «un significativo mutamento di prospettiva che sposta il focus normativo sulla gestione del rischio e sulla responsabilità, anche in termini di capacità di provare l'efficacia delle soluzioni adottate a tutela dei diritti degli interessati (accountability). Il Regolamento, dunque, innova la disciplina in materia di protezione dei dati personali mirando a tutelare i soggetti interessati in una fase prodromica al trattamento. Nello specifico, il legislatore europeo enfatizza il ruolo della valutazione ex ante dei rischi che possono emergere dall'uso di informazioni personali ed accentua le responsabilità degli autori del trattamento (titolare e responsabile del trattamento) rispetto all'adozione delle soluzioni tecniche, logiche e organizzative necessarie ad evitare eventuali situazioni di rischio». Al riguardo cfr. F. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 333-371; F. PIZZETTI, *GDPR e Intelligenza artificiale. Codici di condotta, certificazioni, sigilli, marchi e altri poteri di* soft law *previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire una applicazione proattiva del Regolamento europeo nell'epoca della IA*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University press, Pisa, 2018, pp. 69-97.

[133] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., p. 87 ss. parla di un approccio di "precauzione costituzionale" con una tutela *by design* e *by default*, oltre che *by education*, formando opportunamente sui valori e sui principi coloro che elaboreranno concretamente tali tecnologie.

[134] Comunicazione della Commissione europea «*Piano coordinato sull'intelligenza artificiale*» COM(2018) 795 *final* del 7 dicembre 2018.

[135] Cfr. P. CUCCURU, *op. cit.*, p. 115 ss., secondo cui, in ragione delle esigenze di governabilità e controllabilità da soddisfare, le *blockchains* ibride rappresentano la soluzione più feconda per il futuro.

oppure tecniche atte a prevenire la re-identificazione dei soggetti che non permettano di ricondurre i dati a un solo soggetto o coppie di chiavi diverse per ciascuna transizione[136].

Peraltro, la *distributed ledger technology* e la *blockchain* favoriscono l'integrità e la sicurezza dei dati, la resistenza ad attacchi e il controllo distribuito sugli stessi, in linea con le previsioni in materia di protezione dei dati personali[137]: queste tecnologie garantiscono tali aspetti fin dalla progettazione per impostazione predefinita e, di conseguenza, risultano conformi agli obiettivi perseguiti dagli strumenti previsti dal regolamento europeo 2016/679, come la *data protection by design* e *by default*.

Anche per quanto attiene agli *smart contracts*, al fine di provare a superare i profili di criticità nell'applicazione della disciplina civilistica, il diritto può fare leva sulla stessa tecnologia, immaginando di incorporare all'interno del codice informatico clausole, misure correttive e strumenti rimediali proattivi e reattivi, al fine di regolare le eventuali responsabilità in caso di problematiche e di errata programmazione del codice, e, altresì, meccanismi che permettano di inibire l'esecuzione a seguito di un provvedimento del giudice[138]. In via esemplificativa alcune *blockchains* prevedono la funzione di autodistruzione "*kill switch*" o "*self destruct*", disciplinata dalle parti, al fine di garantire l'attuazione di eventuali pronunce di risoluzione, nullità o annullabilità dello *smart contract*[139]; parimenti possono essere implementate funzioni di modifica del contenuto del codice informatico, laddove si renda giuridicamente necessario. Un altro strumento è costituito dalle operazioni *multi-signature* (*multi-sig*), che prevedono un meccanismo di risoluzione delle controversie, avvalendosi di un utente terzo interno al sistema con funzione di arbitro[140].

Con l'incorporazione del diritto nella tecnica si coniuga anche l'esigenza posta dalle tecnologie emergenti di contrastare l'opacità di potenziali *black box* e diminuire la congenita "asimmetria algoritmica" che le caratterizza[141].

Al riguardo, infatti, insieme alla tecnologia in cui implementare il diritto, è necessario affidarsi a una trasparenza sostanziale nei confronti degli utenti e, parallelamente, consentire la conoscenza della logica

---

136 Si tratta di tecniche quali le *multi-party computation*, *ring signatures*, *one-time accounts*, etc. Misure capaci di ovviare all'immutabilità unilaterale e idonee a prevenire la re-identificazione dei soggetti conducono inevitabilmente a rinunciare, almeno parzialmente, ad aspetti costitutivi della tecnologia, che ne determinano anche le potenzialità; cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.; A. PALLADINO, *op. cit.*, p. 155 ss.; F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 89 ss.

137 Cfr. A. GAMBINO, C. BOMPREZZI, *op. cit.*, p. 619 ss.

138 Cfr. L.A. DIMATTEO, C. PONCIBÒ, *Quandary of Smart Contracts and Remedies: The Role of Contract Law and Self-Help Remedies*, in *European Review of Private Law*, fasc. 6, 2019, pp. 805-824.

139 Così F. SARZANA DI S. IPPOLITO, M. NICOTRA, *op. cit.*, p. 111 ss.

140 Cfr. P. CUCCURU, *op. cit.*, p. 109 ss.

141 Al riguardo cfr. C. ACCOTO, *Il mondo dato. Cinque brevi riflessioni di filosofia digitale*, Milano, 2017, p. 66 ss., secondo cui «si va verso la presa di consapevolezza della necessità di un'accountability e di un auditing degli algoritmi (cioè di una conoscenza responsabile, condivisa e più trasparente)» (p. 67); F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge and London, 2015; D. CARDON, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei* big data, Milano, 2016, p. 68 ss.; L. BOLOGNINI, *Follia artificiale. Riflessioni per la resistenza dell'intelligenza umana*, Soveria Mannelli, 2018, p. 47.

degli algoritmi, accompagnata dalla consapevolezza in merito alle conseguenze e all'impatto sulla persona: si tratta di garantire una declinazione rafforzata della trasparenza, ossia il diritto alla conoscibilità, alla comprensibilità e alla sindacabilità, rendendo gli algoritmi oggetto della piena cognizione e del pieno sindacato dal parte del giudice[142]. In tal modo la tecnologia può mantenere e rispettare la sua funzione di strumento "servente" rispetto all'essere umano e alle sue decisioni, soprattutto laddove incidano su diritti e libertà[143].

In tal caso risulta significativo quanto previsto dalla disciplina in materia di *data protection*, che tra le informazioni da fornire all'interessato, per le quali può essere esercitato il diritto di accesso, in caso di processo decisionale automatizzato prevede informazioni significative sulla logica utilizzata, sull'importanza e sulle conseguenze previste del trattamento per l'interessato, cui si coniuga il diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione[144].

Nel caso dell'intelligenza artificiale, l'esigenza di trasparenza si traduce nella necessità di fornire informazioni e garantire l'accesso in merito alla logica degli algoritmi, all'impatto e alle conseguenze per la persona e, altresì, di assicurare l'intervento umano e la contestazione della decisione. Tale approccio permette di confinare o quanto meno di rilevare errori, *bias*, manipolazioni, riequilibrando l'asimmetria tra le parti, al fine di garantire la consapevole autodeterminazione e la correlata libertà degli individui, valori protetti dalla normativa e, più ampiamente, dagli ordinamenti democratici.

Di conseguenza, nei confronti dell'intelligenza artificiale devono essere attribuiti e riconosciuti il diritto alla comprensibilità, capace di informare e rendere consapevole l'interessato, e il diritto alla contestabilità, idoneo a consentire all'interessato, anche per mezzo di un giudice, di valutare e di sindacare la decisione a cui porta la soluzione di intelligenza artificiale. Tali diritti si traducono più ampiamente nel diritto del singolo di sapere se sta interagendo con una macchina e nel mantenere la propria autonomia e autodeterminazione nei confronti della stessa: questo diritto comporta la trasparenza e la comprensione dei meccanismi di funzionamento[145]. Al riguardo la criticità scaturisce dalla natura stessa degli algoritmi, che non seguono una logica basata sul nesso di causalità e, di conseguenza, talvolta possono rendere concretamente difficile garantire questi diritti[146].

---

142 Cfr. S. CRISCI, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici"*, cit., p. 383 ss.

143 In tal senso A. SIMONCINI, *Profili costituzionali della amministrazione algoritmica*, cit., p. 1149 ss., secondo cui, però, quando viene inserito un automatismo decisionale in un procedimento deliberativo, l'automatismo tende ad attrarre la decisione, rendendo difficile prescinderne e rendendo nella pratica "servo" l'uomo, che ne è teoricamente "padrone".

144 Artt. 13, 14, 15 e 22, reg. (UE) 2016/679. In merito cfr. R. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contratto e impresa*, fasc. 3, 2019, pp. 861-894.

145 Cfr. A. D'ALOIA, *op. cit.*, p. 7.

146 Cfr. A. SIMONCINI, S. SUWEIS, *op. cit.*, p. 97 ss. Al riguardo F. COSTANTINO, *Lampi. Nuove frontiere delle decisioni amministrative tra* open *e* big data, in *Diritto amministrativo*, fasc. 4, 2017, p. 799 ss. evidenzia che i modelli utilizzati attualmente sono opachi, non regolati e incontestabili e, peraltro, possono essere errati, dando luogo a gravi lesioni dei

Il riconoscimento del diritto alla comprensibilità e alla contestabilità trova conferma in ambito pubblico nell'esaminata sentenza del Consiglio di Stato, sez. VI, 8 aprile 2019, n. 2270, secondo cui al cittadino «non può essere precluso di conoscere le modalità (anche se automatizzate) con le quali è stata in concreto assunta una decisione destinata a ripercuotersi sulla sua sfera giuridica» e questo implica «la necessità di assicurare che quel processo, a livello amministrativo, avvenga in maniera trasparente, attraverso la conoscibilità dei dati immessi e dell'algoritmo medesimo. In secondo luogo, conseguente al primo, il giudice deve poter sindacare la stessa logicità e ragionevolezza della decisione amministrativa robotizzata, ovvero della "regola" che governa l'algoritmo».

Si tratta, di conseguenza, di garantire una "trasparenza algoritmica", che impone al titolare il dovere di governare l'algoritmo e le strutture logiche del suo funzionamento per far fronte alle legittime istanze di conoscenza e di protezione dei diritti da parte degli utenti in forza del diritto di conoscere, comprendere e sindacare il sistema di intelligenza artificiale: in tal modo agli individui sono assicurate la consapevole autodeterminazione, la possibilità concreta di controllo e un'autentica libertà[147].

Anche nel caso della *blockchain* e degli *smart contracts*, emerge l'esigenza di garantire il diritto alla comprensione e alla spiegabilità e, di conseguenza, il diritto alla sindacabilità e alla contestabilità da parte degli interessati e del giudice.

Il fatto che il "contratto intelligente" sia costituito da stringhe di codice informatico, infatti, da un lato, ne rende difficile la predisposizione, ancor più ostica in caso di clausole generali e principi interpretabili, con il pericolo concreto di divergenze tra l'accordo tra le parti e la traduzione nell'algoritmo e, dall'altro, una volta formato, lo rende difficilmente intellegibile nel suo contenuto. Il riconoscimento del diritto alla comprensibilità e alla contestabilità, di conseguenza, è necessario per permettere di applicare pienamente le norme civilistiche di riferimento e per evitare asimmetrie tra chi gestisce queste soluzioni e chi se ne serve, che siano le parti di uno *smart contract* o il giudice: questi diritti possono declinarsi in tale contesto anche nell'esigenza concreta di un "interprete" del linguaggio contrattuale.

L'approccio proattivo e preventivo di incorporazione del diritto nella tecnica, accompagnato dal diritto alla comprensibilità e alla contestabilità, si traduce nelle tecnologie emergenti anche nella necessità di abbracciare una logica di *accountability* e responsabilizzazione dei soggetti che gestiscono tali tecnologie, accompagnata dalla definizione delle rispettive responsabilità, dall'attenzione alla sicurezza, dall'effettività e dall'efficacia del sistema sanzionatorio correlato. Anche in questo caso tale approccio è presente nel

diritti: le decisioni, infatti, sono adottate in base ad un numero talmente elevato di dati «da rendere praticamente impossibile la ricostruzione a posteriori dell'*iter* logico, e quindi della motivazione, con ovvi riflessi sul diritto di difesa di chi si ritenesse pregiudicato».

147 Cfr. S. LEUCCI, *Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca*, in *Rivista di diritto dei media*, fasc. 1, 2017, p. 123 ss.

regolamento europeo 2016/679 in materia di *data protection*[148].

Questa esigenza emerge in caso di *blockchain* e *smart contract*, dove è necessario individuare forme di tutela che consentano l'individuazione dei soggetti (si pensi alle figure del titolare e del responsabile previste dalla disciplina in materia di *data protection*) e l'attribuzione delle connesse responsabilità: al riguardo, come già detto, si può ipotizzare di incorporare all'interno del codice informatico misure correttive e strumenti rimediali, al fine di regolare le eventuali responsabilità in caso di problematiche.

Nel caso dell'intelligenza artificiale il problema sorge dal momento che tali tecnologie possono creare danni con il loro comportamento, che può essere difficilmente prevedibile e può scaturire dalla scelta in situazioni eticamente complesse, si pensi alle armi e ai veicoli autonomi. In caso di errori o *bias* è difficile individuare la responsabilità ed emerge il problema se la responsabilità sia ascrivibile sempre e soltanto ad un soggetto umano, quale il programmatore, o se invece talvolta gli algoritmi da soli conducano a decisioni che possono provocare danni. Anche volendo considerare condivisibilmente l'autonomia dell'intelligenza artificiale come meramente operativa, priva pertanto di una coscienza autonoma[149], sicuramente le categorie e le norme giuridiche in tema di responsabilità vivono tensioni e possono risultare insufficienti e inadeguate a regolare un fenomeno inedito[150].

Proprio a causa dell'acquisizione di sempre maggiore autonomia, l'Unione europea si interroga in merito all'eventuale attribuzione di soggettività e al relativo riconoscimento della personalità giuridica alle applicazioni di intelligenza artificiale; gli ordinamenti giuridici cominciano a chiedersi se la macchina non sia soltanto oggetto di diritti, ossia strumento nelle mani di umani, ma possa diventare anche soggetto di diritti.

Il Parlamento europeo nelle «*raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*» del 16 febbraio 2017 parla di "sistemi agenti", nella consapevolezza della futura necessità di attribuire un'imputabilità autonoma in considerazione del sempre più difficile collegamento tra le attività delle macchine e la responsabilità umana. La risoluzione affronta la questione con le categorie giuridiche dei sistemi di assicurazione obbligatoria e forme di responsabilità oggettiva, ma al riguardo auspica il riconoscimento dello *status* giuridico specifico di personalità elettronica, seppur tale riconoscimento non sia scevro di conseguenti complesse problematiche, quali la correlata attribuzione di diritti e doveri e

[148] In specifico artt. 24, 26, 32, 82-84, reg. (UE) 2016/679.

[149] Risoluzione del Parlamento europeo del 16 febbraio 2017 recante «*raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*»: nella "Carta della Robotica", approvata con la risoluzione, viene trattata esplicitamente la questione dell'autonomia decisionale delle macchine. Cfr. D. AMOROSO, G. TAMBURRINI, *I sistemi robotici ad autonomia crescente tra etica e diritto: quale ruolo per il controllo umano?*, in *BioLaw Journal*, fasc. 1, 2019, p. 35 ss.

[150] Cfr. A.C. AMATO MANGIAMELI, *op. cit.*, p. 107 ss.; A. D'ALOIA, *op. cit.*, p. 11 ss.; G. DE ANNA, *Automi, responsabilità e diritto*, in *Rivista di Filosofia del diritto*, fasc. 1, 2019, p. 124 ss., che argomenta in merito al rischio di erosione della responsabilità in caso di automatizzazione dei processi decisionali.

l'individuazione della capacità di agire[151].

Al riguardo l'incorporazione del diritto nella tecnica può acquisire il volto dell'attribuzione di soggettività e responsabilità alla macchina stessa.

4. Conclusioni

Le problematiche giuridiche aperte e la necessità di rispettare i valori giuridici di riferimento evidenziano l'importanza della capacità umana di orientare intelligenza artificiale, *blockchain* e *smart contract* e, più ampiamente, la tecnologia, che dipende strettamente dall'abilità di coordinare le diverse competenze necessarie e dalla capacità di regolazione.

L'incidenza delle tecnologie informatiche sul diritto è particolarmente significativa e conduce a riflessioni sul rapporto tra tecnologia e diritto e sulla regolamentazione giuridica di tali fenomeni.

In base all'analisi svolta, la direzione può essere quella di incorporare il diritto nella tecnica, in modo che davvero si realizzi l'incisiva locuzione di Lessig "*code is law*", che evidenzia l'aspetto regolatorio insito nel codice informatico[152]: propriamente *code is law* solo quando il diritto, assolvendo alla sua funzione preventiva di regolazione, incorpori nel linguaggio macchina il rispetto dei principi e delle norme. Questo approccio preventivo e proattivo di incorporazione del diritto nella tecnica può essere proficuamente accompagnato dall'attribuzione del diritto alla comprensibilità e alla contestabilità della tecnologia e da una logica di responsabilizzazione dei soggetti.

Tale logica permette di rispondere all'esigenza di tutela della persona rispetto alla tecnologia, che anima fin dal suo avvento il diritto dell'informatica e che si declina nella protezione dei dati personali rispetto ad algoritmi e automatismi.

Il diritto dell'informatica sorge dalle problematiche giuridiche sollevate dall'impatto e dalla diffusione delle tecnologie informatiche e si caratterizza per alcune peculiarità, quali l'intangibilità dell'oggetto[153], il superamento dei confini territoriali dal punto di vista dello spazio, la trasversalità e la globalizzazione dei problemi oggetto di disciplina.

---

1. [151] Sugli agenti software come soggetti di diritto cfr. G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contratto e impresa*, fasc. 2, 2002, pp. 465-499. Sulla responsabilità e sull'*accountability* relative ai sistemi di intelligenza artificiale cfr. M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e* accountability. *Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, pp. 333-371; L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, fasc. 4, 2018, pp. 713-739; G. CAPILLI, *Responsabilità e robot*, in *La Nuova giurisprudenza civile commentata*, fasc. 3, 2019, pp. 621-631; G. COMANDÉ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, fasc. 1, 2019, pp. 169-188; U. RUFFOLO, *Intelligenza Artificiale,* machine learning *e responsabilità da algoritmo*, in *Giurisprudenza italiana*, 2019, pp. 1689-1704.

[152] L. LESSIG, *Code and Other Law of Cyberspace*, New York, 1999.

[153] Cfr. V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2003, p. 89 ss.

L'assenza di barriere territoriali comporta che le risposte giuridiche non possano più limitarsi ai confini nazionali[154], ma debbano, parallelamente alle vicende che sono chiamate a regolare, assumere una veste di *governance* sovranazionale per poter essere pienamente efficaci e non generare altrimenti una tensione inevitabile tra la dimensione globale delle questioni e il carattere territoriale delle norme da applicare; tale tensione è presente nel rapporto tra la norma italiana dedicata alle *distributed ledger technologies* e agli *smart contracts* e la regolazione europea di riferimento.

In prospettiva futura la vocazione transnazionale delle tecnologie emergenti porta a ritenere opportuna una regolamentazione sovranazionale, capace di governare in modo effettivo ed efficace un fenomeno che ontologicamente supera i confini dei singoli Stati, eventualmente integrata da regolazioni nazionali, al fine di evitare un'autoregolazione pericolosa in quanto capace di creare *de facto* un ordinamento parallelo rispetto a quello giuridico[155]. In considerazione dell'oggetto da disciplinare, dovrebbe trattarsi di una regolamentazione atta a contenere i principi giuridici di riferimento, idonei a tutelare i diritti e prevenire i conflitti, rinviando a fonti secondarie e standard la regolazione di dettaglio che necessariamente avrà carattere tecnico.

Il diritto è chiamato ad evolvere, dal momento che le tecnologie emergenti chiedono alla regolazione giuridica di svolgere una funzione preventiva efficace, evitando così l'insorgere di conflitti e conseguenti contenziosi[156]. In questa complessa età di trasformazione è in gioco la capacità del diritto di regolare la realtà di riferimento, guidando e indirizzando le tecnologie emergenti verso i valori fondamentali, le libertà e i diritti dei soggetti: è cruciale mantenere il ruolo dell'uomo come guida e quello della tecnologia come strumento nelle sue mani, evitando il realizzarsi di inquietanti visioni tecno-deterministe dove la macchina si sostituisce alla decisione umana[157].

Per riuscire in questo scopo, in conformità al mutamento potenzialmente *disruptive* a livello sociale ed economico determinato dalle tecnologie emergenti, è necessario un approccio giuridico consono e parimenti *disruptive* a tali fenomeni[158], capace di determinare al tempo stesso un saggio equilibrio fra gli estremi contrapposti di estensioni eccessive e restrizioni soffocanti, fra le quali da sempre oscilla l'evoluzione tecnologica[159].

---

154 Sui cambiamenti profondi che investono lo Stato nella società tecnologica cfr. L. CASINI, *Lo Stato nell'era di Google*, in *Rivista trimestrale di diritto pubblico*, fasc. 4, 2019, p. 1111 ss.

155 Cfr. M. GIULIANO, *op. cit.*, p. 989 ss. Sulle potenzialità dello spazio giuridico europeo cfr. F. CIARAMELLI, *Lo spazio giuridico europeo e le sue potenzialità politiche*, in *RIFD. Rivista internazionale di filosofia del diritto*, 2015, fasc. 1, pp. 171-175.

156 Al riguardo cfr. M. PIETRANGELO, *Il diritto e le tecnologie informative: qualche proposta per il nuovo millennio*, in G. PERUGINELLI, M. RAGONA (a cura di), *L'informatica giuridica in Italia. Cinquant'anni di studi, ricerche ed esperienze*, Napoli, 2014, p. 621 ss., che auspica per il diritto «un ruolo attivo, ma *leggero*, privo di peso» (p. 623).

157 Cfr. R. BORRUSO, *op. cit.*; G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, cit., p. 831 ss.

158 G. FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, cit., p. 441 ss.; M. GIULIANO, *op. cit.*, p. 989 ss.

159 In tal senso R. BORRUSO, *op. cit.*

Una strada per raggiungere questi obiettivi è costituita da una nuova relazione tra diritto e tecnica, che incorpori il primo nella seconda, valorizzando in tal modo la costruzione del diritto stesso come scienza che nasce per conferire certezza alle relazioni umane, attribuendo diritti e doveri, riuscendo a tutelare la persona e la società rispetto alla tecnologia[160]. Il valore della certezza del diritto non può essere smarrito a causa dell'evoluzione impressa dalle tecnologie emergenti e per realizzarsi può fare leva sull'incorporazione del diritto nella tecnica, accompagnata dal diritto alla comprensibilità e alla contestabilità della tecnologia e dalla responsabilizzazione degli esseri umani[161].

[160] Cfr. E. MAESTRI, *op. cit.*, p. 173 ss., secondo cui la sfida normativa consiste «nel realizzare una continua interazione tra regolazione statuale o sovranazionale e l'architettura del *code*» (p. 174).
[161] Cfr. L. VIOLA, *Combinazione di dati e prevedibilità della decisione giudiziaria*, in *Diritto di Internet. Digital Copyright e Data Protection*, fasc. 1, 2019, p. 216.